SERMAYE PİYASASI KURULU
ARACILIK FAALİYETLERİ DAİRESİ

FİNANSAL SEKTÖRDE YIKICI YENİLİK: DAĞITILMIŞ DEFTER TEKNOLOJİSİ VE TÜRKİYE SERMAYE PİYASALARININ DURUMU (DISTRIBUTED LEDGER TECHNOLOGIES/BLOKCHAIN)

YETERLİK ETÜDÜ

Burak GÖRMEZ
Bilişim Uzman Yardımcısı

Temmuz 2017
ANKARA

YÖNETİCİ ÖZETİ

Ülkelerin kalkınma süreçlerinde oldukça önem arz eden faktörlerden biri olarak karşımıza çıkan inovasyon ve yenilikçi sistemler günümüzde birçok ülkenin ilgi gösterdiği konulardandır. Modern iktisat teorilerinin odak noktasını oluşturan ve ülkelerin rekabet gücünün, iktisadi büyüme ve kalkınma süreçlerinin en önemli faktörlerinden biri olarak kabul edilen inovasyona yönelik iktisadi girişimler ve faaliyetler özellikle 1980 yılından itibaren artmaya başlamıştır.

1995 yılında Harvard Business Review dergisinde Bower ve Clayton Christensen tarafından yayınlanan "Yıkıcı Teknolojiler: Dalgayı Yakalama" isimli makale iş dünyasına, piyasanın en alt seviyesinden giriş yapan bir ürün veya hizmetin hızla yaygınlaşıp yükselmesi sonucu piyasaya hâkim olan diğer ürün veya hizmetin ortadan kaldırılmasını ifade eden yıkıcı inovasyon kavramını getirmiştir.

Günümüzde hızla değişen teknolojilerin ve gelişen koşulların bir sonucu olarak ihtiyaçlarda farklılaşmakta ve gelişime yön vermektedir. Öyle ki sanayi devriminde insanın kas gücünün makinelere bırakılmasının devamında yaşadığımız dönemde, nesnelerin interneti (IoT), endüstri 4.0, büyük veri depolama ve analitiği teknolojileri ile insanın algılama, yorumlama ve karar verme kabiliyeti dijital nesnelere devredilmiştir. Bilgiye hızlı erişim ve işleme imkanı veren, ayrıca fiziksel kısıtlamaları ortadan kaldıran teknolojik gelişmeler yeni doğan teknolojilerin, doğrusal bir süreçten çıkıp eksponansiyel bir yayılımla ilerlemesini sağlamaktadır. Bu süreçte eksponansiyel dönüşüm hızını yakalayabilen şirketler rekabette büyük bir avantaj yakalarken, dönüşümde hantal kalan şirketler ise yeni teknolojinin yıkıcı gücünden kurtulamamaktadır. Yıkıcı etkilerin hissedilmeye başlandığı noktada ise yerleşik firmalar tarafından piyasadaki statünün korunması amacıyla yeni ürünün üretim haklarının veya firmasının satın alınması, yerleşik ürününün kısmen ücretsiz sunulması, maliyet azaltıcı çalışmalar yapılması ve promosyonlar düzenlenmesi gibi karşı stratejiler uygulanabilmektedir.

Teknolojide yaşanan bu değişim sermaye piyasalarını da etkilemeye devam etmektedir ve özellikle sermaye piyasası altyapı kurumlarının iş modellerini küresel düzeyde ve kısa zamanda önemli bir dönüşüme uğratma potansiyeline sahiptir. Bilginin finansman kadar değerli sayılmaya başlandığı bir ortamda, finansal teknolojinin getirdiği yeni iş modelleri sermaye piyasası katılımcılarını da bu alanda projeler geliştirmeye itmektedir. Bu doğrultuda genellikle yerleşik bankalar ve aracılar gibi hizmet sunucuları tarafından sunulmakta olan finansal hizmetlerin ayrıştırılmasıyla denkler arası borçlanma, kitle fonlaması, akıllı sözleşmeler, robo-tavsiye, sanal para ve dağıtılmış defter teknolojisi gibi finansal hizmetleri kapsayan finansal teknoloji kavramı oluşmuştur.

İhtiyaç duyulan fonların etkin kullanımı faaliyetlerini kapsayan –finans- ve üretim amacıyla geliştirilen araçları ve bilgiyi kapsayan –teknoloji- kelimelerinin bir araya gelmesi ile ortaya çıkan finansal teknoloji (FinTek), finansal sistem için önemi giderek artan kavramlar arasında yer almaktadır. FinTek şirketleri ise finansal

hizmetler endüstrinde yıkıcı güç olarak ortaya çıkmaktadır. Dağıtılmış defter teknolojisi, makine öğrenimi ve yapay zeka gibi gelişmekte olan teknolojilerin, FinTek girişimcilerini ve geleneksel şirketleri desteklemek için kullanılma potansiyeline ek olarak finansal hizmetler sektörünü değiştirme potansiyeli de bulunmaktadır.

Öyle ki teknoloji kullanımı ile blok zinciri, robo-tavsiye uygulamaları ve kitle fonlaması platformları gibi inovatif FinTek iş modelleri, düzenlenmiş bazı faaliyetlerde aracıların ortadan kalkmasına yol açma potansiyeline sahiptir.Kitle fonlaması platformları borsaların, otomatik yatırım tavsiyeleri sunan robo-tavsiye platformları geleneksel danışmanların, kredi veren veya verilmesine aracılık eden uçtan uça borç verme platformları ise bankaların aracılık rollerine talip olmaktadır. Bu durum da, günümüzde ayakta kalmak ve gelişmek isteyen finansal piyasa aktörleri için inovasyonun artık bir seçenekten ziyade zorunluluk olduğunu göstermektedir.

Diğer taraftan, inovasyonun ve finansal hizmetler endüstrisinin geleceği için etkili regülasyonlara olan ihtiyaç artmakta ve regülatörler açısından FinTek'lere zarar vermeden, ancak aynı zamanda finansal sistemi güvence altına alarak FinTek sektörünün nasıl düzenlenebileceği hususu önemli olmaktadır. Çünkü FinTek regülasyonu, değişen finansal hizmetler dünyasında tutarlı bir manzara oluşturabilmenin temel taşıdır. FinTek regülasyonlarının, regülasyonun özellikle geleneksel olmayan finansal hizmet şirketlerinin sisteme girişi için kolaylık sağlama veya engel olma potansiyeli olduğu göz önüne alınarak yapılması gerekmektedir.

FinTek kategorilerinden sermaye piyasalarında, özellikle sermaye piyasası altyapı kurumlarının iş modellerinde, önemli derecede yıkıcı etki yaratma potansiyeline sahip olma hususunda blok zinciri/DLT öne çıkmaktadır.

Blok zinciri/DLT, finansal aktörler arasındaki veri işleme ve paylaşma eylemlerini kolaylaştırmak için fikir birliği protokolleri ile her güncelleme hakkında mutabakat sağlanan dağıtılmış veri tabanı sistemidir. Bilgisayar biliminin ve kriptografinin çeşitli alanlarından kavramlar ise, bu sistemi gerçekleştirebilmek için kullanılmaktadır. Blok zinciri/DLT kullanımı ile aracıların sayılarının azaltılması ve mutabakat sürecinin daha verimli hale getirilmesi suretiyle bazı finansal işlemlerin takas ve takas öncesi işlemler sürecinin hızlandırılması sağlanabilir. Özellikle de Blok zinciri/DLT, fazla aracıya olan ihtiyacı azaltarak tarafların ülkeler arasında birbirleri ile daha kolay işlem yapmasını sağlayabilir. Blok zinciri/DLT ağının tüm katılımcılarının ağın kalanı ile tutarlı olacak şekilde kayıtların lokal kopyasını elinde tutması ve işlemlerin onaylanması için fikir birliği algoritmalarını kullanması anlamına gelen blok zincirinin dağıtılmış mimarisi sayesinde, mutabakat süreci daha hızlı ve verimli şekilde yapılabilir.

Öte yandan, Blok zinciri/DLT sisteminin yukarıda açıklanan olası faydalarına ulaşılabilmesi için öncelikle teknoloji ile ilgili siber risk, dolandırıcılık ve kara para aklama gibi bazı potansiyel risklerin ve yönetim, gizlilik, regülasyon, ölçeklenebilirlik, mevcut sistemlerle ve farklı ağlarla birlikte çalışabilirlik gibi muhtemel birçok zorluğun üstesinden gelinmesi gerekmektedir.

İÇİNDEKİLER

KISALTMALAR CETVELİ

AB	:	Avrupa Birliği
AIFMD	:	Alternative Investment Fund Managers Directive
ASIC	:	Australian Securities and Investments Commission
CPU	:	Central Processing Unit
CSD	:	Central Securities Depositories Regulation
CSDR	:	Central Securities Depositories Regulation
DVP	:	Delivery Versus Payment
EMIR	:	European Market Infrastructure Regulation
ESMA	:	European Securities and Markets Authority
Eurostat	:	Statistical Office of the European Communities
FATF	:	Financial Action Task Force on Money Laundering
FCA	:	Financial Conduct Authority
FinTek :	:	Finansal Teknoloji
FSB	:	Financial Stability Board
G-20	:	Group of Twenty
IOSCO	:	International Organization of Securities Commissions
IoT :	:	Internet of things
MiFID	:	Markets in Financial Instruments Directive
MiFIR	:	Markets in Financial Instruments Regulation
MKT	:	Merkezi Karşı Taraf
MSK	:	Merkezi Saklama Kuruluşu
NASA	:	National Aeronautics and Space Administration
NIST	:	National Institute of Standards and Technology
NSA	:	National Security Agency
OECD	:	Organization for Economic Co-operation and Development
OTC	:	Over-The-Counter
PoS	:	Proof of Stake
PoW	:	Proof of Work

RSA	:	Right Shift Algorithm
SFD	:	The Settlement Finality Directive
SFTR	:	Securities Financing Transactions Regulation
SHA	:	Secure Hash Algorithm
SHS	:	Secure Hash Standart
SPKn	:	6362 sayılı Sermaye Piyasası Kanunu
SPV	:	Simplified Payment Verification
UCITS	:	Undertaking for Collective Investment in Transferable Securities

TABLO VE ŞEKİLLER CETVELİ

Şekiller

Tablolar

1. GİRİŞ

Teknolojik gelişmelerin finansal sisteme yansımaları olduğu günümüzde, küresel bağlantı ile ürün ve hizmetlere daha geniş tabanlı erişimi kolaylaştıran teknoloji, finansal sistemin gelişmediği ülkelerde tabana yayılmanın artmasına, geleneksel kaynaklardan finansman sağlama imkânı bulamayan gerçek ve tüzel kişilerin yeni aracılardan kaynak edinme imkânına kavuşmasına ve hizmetlerin maliyetinin düşmesine hatta bazı durumlarda ortadan kalkmasını katkı sağlamaktadır.

Öyle ki teknoloji kullanımı ile,

- Kitle fonlaması platformları, daha önceleri yüksek gelirli yatırımcılara ayrılan sermaye yatırımlarına bireysel yatırımcıların da erişmesini,

- Robo-tavsiye uygulamaları daha önce kurumsal ve özel bankacılık müşterileri için mümkün olan modern portföy teorisine dayalı yatırımları bireysel yatırımcıların da gerçekleştirmesini,

- Belirli sosyal alım satım platformları ise sıfır komisyon ile işlemlerin yapılabilmesini

mümkün hale getirmiştir. FinTek ise bu eğilimin bir tezahürüdür.

Blok zinciri teknolojisi, robo-tavsiye, P2P kredi, kitle fonlaması ve mobil ödeme gibi kategoriler üzerine yoğunlaşan önemli gelişmelerle birlikte FinTek kavramı dünya genelinde yoğun ilgi görmekte ve finansal sistemi çeşitli kanallardan etkilemektedir. Menkul kıymetlerin kâğıt sertifikalar halinde ihraç edilmesinin ve saklanmasının bırakılıp kaydi sistemlere geçilmeye başlanması sayesinde genel olarak maliyetleri düşüren Fintek'lerin de yaygınlaşmasıyla aracıların ortadan kalkması ve yerini teknolojik çözümlerin alması da gündeme gelmektedir.

FinTek sektörünün her geçen gün büyümesi ve finansal hizmetler endüstrisini dönüştürme potansiyelinin artması, finansal hizmetler endüstrisinin geleceği için etkili regülasyonlara olan ihtiyacı artırmaktadır.

Bu noktada FinTek'lerin nasıl düzenleneceği hususu önemli olmaktadır. Çünkü FinTek regülasyonunun, özellikle geleneksel olmayan finansal hizmet şirketlerinin sisteme girişi için kolaylık sağlama veya engel olma potansiyeline sahip olması nedeniyle iki tarafın keskin kılıca benzetilmesi mümkün olup regülasyonların da bu çerçevede yapılması gerekmektedir.

FinTek kategorilerinden bazılarının, veri paylaşımı gibi süreçlerden dolayı yapısal olarak birbiri ile etkileşime girme ihtiyacı olan aktörlerden oluşan sermaye piyasalarında, belirli iş modelleri üzerinde yıkıcı etki yaratma potansiyeli bulunmaktadır. Finansal aktörler arasındaki veri işleme ve paylaşma eylemlerini kolaylaştırmak için bir yöntem önermekte olan DLT ise bu alanda yıkıcı etkilere sahip olma bağlamında öne çıkmaktadır.

Blok zinciri, çoğunlukla Bitcoin protokolünün temelindeki teknoloji olarak bilinmekte olup, daimi ve değişmez kayıtların oluşturulabilmesi için kriptografik olarak imzalanmış verilerin bloklara eklenmesi sürecini tanımlamak için kullanılmaktadır. Dağıtılmış defter teknolojisi ise, sistemdeki tüm düğümlerin paylaşılan bir verinin doğru versiyonu üzerinde fikir birliğine varmak için çalıştığı veri tabanı sistemini tanımlamak için kullanılan bir terimdir. Bu amaca ulaşmak için, bütün dağıtılmış defter teknolojileri tarafından blok zincirinin kullanılması zorunlu değildir. Bununla birlikte bu çalışmanın amacı doğrultusunda, sermaye piyasalarında kullanılan dağıtılmış defter teknolojilerinin blok zinciri teknolojisinin çeşitleri olacağı varsayılmakta, bu nedenle de çalışmada DLT ve blok zinciri terimleri birbirinin yerine kullanılmaktadır.

Bu çalışmada, sermaye piyasalarındaki dijital dönüşüm, bu dönüşüm sonucunda ortaya çıkan FinTek kategorileri ve özellikle dağıtılmış defter teknolojisi ile sermaye piyasaları üzerindeki olası yıkıcı etkileri üzerinde durulmaktadır. Birinci bölümde, genel olarak FinTek ve özelde DLT alanında yaşanan gelişmelerin yıkıcı etkilerinin daha iyi anlaşılmasını teminen, yıkıcı inovasyondan kısaca bahsedilmektedir. İkinci bölümde, FinTek kavramı ve sermaye piyasalarına etkisinden söz edilmekte; üçüncü bölümde ise bir bütün olarak dağıtılmış defter teknolojisi ve özellikleri hususu üzerinde durulmaktadır. Dördüncü bölümde, menkul kıymet piyasalarına uygulanan DLT'nin olası faydalarından bahsedilmektedir. Beşinci ve altıncı bölümde, genel olarak DLT uygulamalarının olası zorlukları ve riskleri üzerinde durulmakta; nihayet son bölümde, DLT'nin mevcut AB ve Türkiye düzenleyici çerçevesinde nasıl ele alınabileceğine değinilmektedir.

2. YIKICI YENİLİK KAVRAMI

2.1 İnovasyon/Yenilik Kavramı

"İnovasyon" kelimesi, yenilenmek veya değiştirmek anlamına gelen Latince kökenli innovare fiilinden ve innovatus (inno+vatus) isminden türetilmiştir. Böylece, novice (çırak), renovation (yenileme) ve novelty (orijinalite) gibi diğer İngilizce kelimelerin de Latince novus'dan türediği söylenebilir (Adair 2008: 105).

Ekonomist ve politika bilimcisi Joseph Schumpeter'ın 1911'de yazdığı ve 1934 yılında İngilizce'ye çevrilen kitabında, müşterilerin henüz bilmediği bir ürünün veya var olan bir ürünün yeni bir niteliğinin pazara sürülmesi; yeni bir üretim yönteminin uygulanmaya başlanması; yeni bir pazarın açılması; hammaddelerin veya yarı mamullerin tedariği konusunda yeni bir kaynağın bulunması; bir sanayinin yeni organizasyona sahip olması olarak tanımlanan İngilizce 'innovation' sözcüğünün karşılığı olarak Türkçe'de "yenilik/yenilikçilik" kavramı kullanılmaktadır. Ancak yenilik ve benzeri kavramlar, "innovation" ile ifade edilmeye çalışılanı tam anlamıyla ifade etmemektedir. Çünkü inovasyon kavramının özünde, yeni olarak tanımlanan şeylerin toplumsal ve ekonomik değişime dolayısıyla da faydaya dönüştürülmesi yatmaktadır. Türkçe olarak ifade edilen yenilik kavramı içerisinde de bu vurgunun çok fazla belirgin olmadığı görülmektedir (Uzkurt 2008: 17). İnovasyon, yeniliğin kendisinden çok sonucunu; farklılaştırmaya ve değiştirmeye bağlı ekonomik ve toplumsal bir sistemi ifade eder. Dolayısıyla bir bütün olarak ele alındığında inovasyon kavramı, yenilikle aynı yoldan giden ve fakat sonuçları itibariyle ondan ayrılan bir başka kavramlaştırmayı ifade edicidir. Öte yandan inovasyonun ruhunda olan,

- Özgünlük ve ayırt edicilik,
- Yaratıcı bir sürecin sonucu olma,
- Tüketici veya toplum tarafından değerli bulunan cazip bir çözüm yaratma,
- Gerçek ve sürdürülebilir bir rekabet avantajı yaratma,
- Pazar ve rekabet üzerinde etkili olma

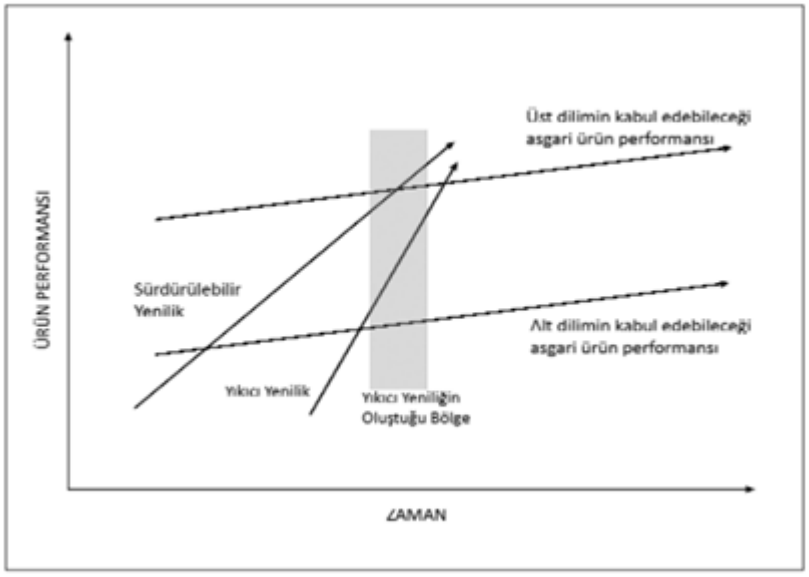
gibi özellikler yalnızca "yenilik" kavramıyla ifade edilememektedir. Bir şeyin yeni olması, bırakın özgün, yaratıcı, ayırt edici ve faydalı olmayı, daha iyi olduğu anlamına bile gelmeyebilir (Özgenç 2009). Görüldüğü üzere, "yenilik" ve "yenilenme", inovasyonla ifade edilmeye çalışılan durumun dışında başka çağrışımlara da yol açtığından bu çalışmada "yenilik" yerine "inovasyon" kavramı kullanılacaktır.

İnovasyonun tanımı konusunda uluslararası düzeyde kabul gören kaynakların başında gelen OECD ile Eurostat'ın birlikte yayınladığı Oslo Manual Kılavuzunda (2005: 46) inovasyon; "süreç olarak, bir fikri pazarlanabilir bir ürün ya da hizmete, yeni ya da geliştirilmiş bir imalat yahut dağıtım yöntemine, ya da yeni bir toplumsal hizmete dönüştürmek" şeklinde açıklanmıştır.

2.2 Yıkıcı İnovasyon Teorisi

Schumpeter'a göre kapitalizmin doğasında yer alan krizler yıkıcı güçleriyle en zayıf firmaları ve aşırı risk alan girişimcileri tasfiye ederken, ayakta kalmayı başaranları da yeniliğe zorlar (Schumpeter, 1943). Yaratıcı Yıkıcılık (creative destruction) olarak adlandırılan bu sistemde girişimci, yenilikçi ve dinamik, yaratıcı ve yıkıcılık görevini yerine getirmektedir. Bu tür paradigmatik değişiklikler, pazara yeni girenlere periyodik olarak mevcut yapıyı değiştirme imkânı vermektedir (Teece ve Coleman, 1998).

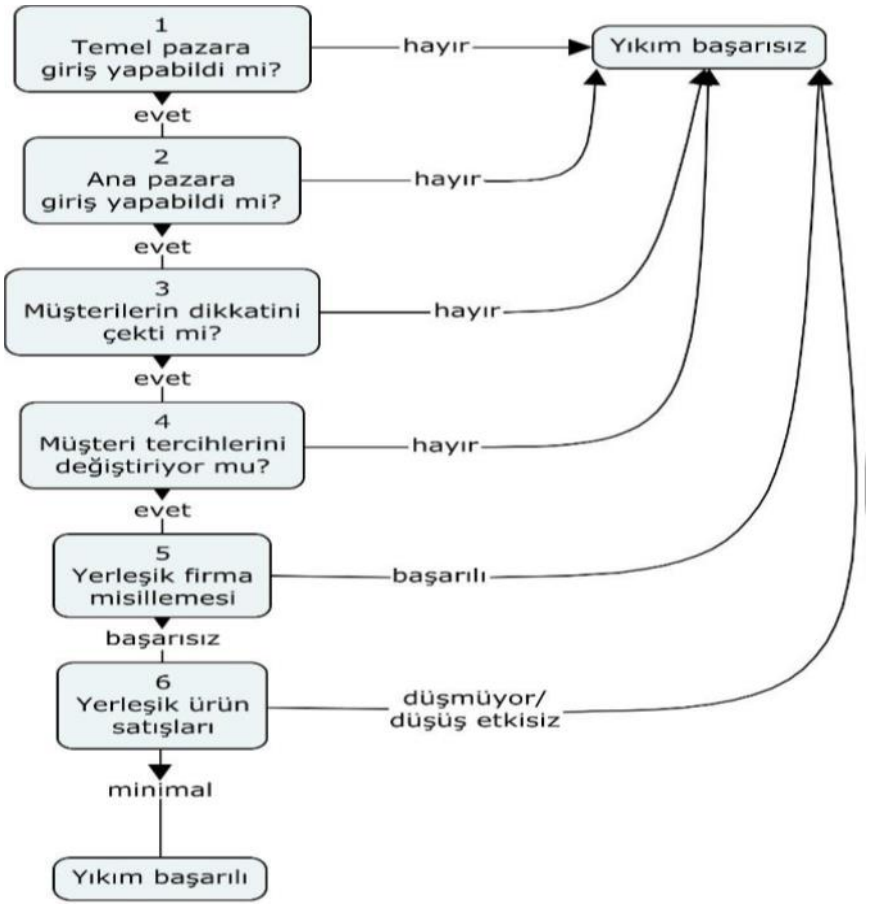
Piyasanın en alt seviyesinden giriş yapan bir ürün veya hizmetin, hızla yaygınlaşıp yükselmesi sonucu piyasaya hâkim olan diğer ürün veya hizmetin ortadan kaldırılması anlamında kullanılan yıkıcı inovasyon teorisi ise temelini Bower ve Christensen'in 1995 yılında Harvard Business Review dergisinde yayınladıkları, "Yıkıcı Teknolojiler: Dalgayı Yakalama" isimli makalesinden alır. Makalede lider firmaların birçok gelişmekte olan teknolojiyi görmezden geldikleri, bunun rehavetten değil firmaların yüksek getirili projelere yönelmesinden kaynaklandığı ifade edilmektedir (Bower ve Christensen, 1995). Teoriye göre firmalar piyasanın üst dilimi yerine alt dilimine yönelerek büyümelidir. Yönelme davranışı ancak firmalar temel işlerinin karlığı en yüksek olduğu noktada eyleme dönüşmelidir. Temel işine çok yoğunlaşan ve mevcut müşteri odaklı yaklaşıma sahip firmalarda yenilik yavaş (incremental innovation) ve mevcut pazarı destekleyicidir (sustaining innovation). Yıkıcı inovasyon (disruptive innovation) ise, farklı olarak, firmanın temel işinden farklı ürünlere ve daha önce müşteri olmamış kullanıcı grubuna yönelmesi ile oluşur. Piyasanın dinamik alt diliminde büyüme fırsatları oturmuş üst dilimden daha fazla olduğundan yıkıcı inovasyon basit ve ucuz ürünlere yoğunlaşır (Bower ve Christensen, 1995).



Şekil 1 (Yıkıcı İnovasyonun Zaman-Performans Grafiği, Bower ve Christensen, 1995)

Şekil 1'de görüldüğü üzere pazarda hem üst hem de alt kademe kullanıcılar tarafından kabul edilebilir ürün performansı zaman içinde artmaktadır. Pazarda, lider firmalar tarafından artan ürün performansı talebine yönelik sürdürülebilir[1] inovasyon faaliyetleri yürütülmektedir. Sürdürülebilir inovasyona yoğunlaşan firmalar yüksek getiriye yoğunlaşmaları nedeniyle alt kademeye yönelik ürünleri üretmemektedir. Diğer taraftan yıkıcı inovasyona odaklanan firmalar basit ve ucuz ürünlere odaklanmakta ve ürünlerini zaman içinde kabul edilebilir ürün performansına taşımaktadırlar. Daha sonra yeterli bilgi birikimine sahip firmalar üst kademenin kabul edebileceği ürünlere yönelmektedir. Şekil 1'deki gri bölge lider firmalar ile yıkıcı inovasyona odaklanan firmaların ürünlerinin rekabete giriştiği yıkıcı inovasyonun oluştuğu bölgedir. Elbette bu süreç yeni yıkıcı inovasyon stratejisini benimseyen firmalar tarafından zorlanacak ve daha önce yıkıcı inovasyon ile piyasa liderliğine oynayan firmalar yeni firmaların tehditleri ile karşılaşacaktır.

Yıkıcı inovasyonun oluşma evrimi ise aşağıdaki şekilde özetlenebilir. (Reagan, 2014)



Şekil 2 (Yıkıcı İnovasyonun Oluşma Evrimi, Reagan, 2014)

[1] Sürdürülebilir inovasyonlar yeni ihtiyaçlara cevap verebilmek için mevcut sistemi yok saymadan sistemin performansını artırma potansiyeline sahip inovasyonlardır. (Christensen, Horn ve Staker, 2013).

Şekil 2 incelendiğinde yıkıcı inovasyonun ilk önce temel pazara giriş yapması ile sürecin başladığı görülmektedir. Temel yeteneklerde düşük düzeyli kullanıcıların olduğu alana giriş yapabilen yıkıcı inovasyon burada gelişip ana pazara giriş yapmaktadır.

Ana pazara girip müşterilerin ilgisini çektiği bu dönem, yerleşik firmanın bu inovasyonu/teknolojiyi fark ettiği zamandır. Müşterilerin yeni ürüne ilgisinin artmaya başladığı ve yerleşik ürün satışlarının azalmaya başladığı bu noktada yerleşik firma piyasadaki statüsünü korumak amacıyla yeni ürünün üretim haklarını veya firmasını satın almak, yerleşik ürünü kısmen ücretsiz sunmak, maliyet azaltıcı çalışmalar yapmak ve promosyonlar düzenlemek gibi piyasa rekabet stratejilerini karşı strateji olarak uygulamaya başlamaktadır. Yerleşik firmanın karşı stratejileri yıkıcı inovasyonu engelleyemediği zaman yıkım gerçekleşmektedir.

2.3 Yıkıcı Teknoloji Örnekleri

2006 yılı başlarında Oracle firması, MySQL firmasının başı çektiği ve alt seviye kullanıcılarına hizmet veren açık kaynak veri tabanı sunucularından rahatsızlık duyduğu için karşı strateji olarak alt seviye kullanıcılarına hizmet veren açık kaynak veri tabanı sunucularından Sleepycat ve InnoDB'yi satın almış ve PHP gibi açık kaynak dillerinin kullanılarak Oracle ürünlerine uygulamalar yazılmasını sağlamıştır. Ardından SUN Microsystems, MySQL firmasını satın almış ve 2010 yılında da ORACLE, SUN firmasını satın almıştır. (Katsamakas & Georgantzas, 2010) Burada ORACLE firmasının yıkıcı yenilik karşısında tehdidi kendi çıkarları doğrultusunda kullanarak başarılı bir strateji uygulamıştır.

3. SERMAYE PİYASALARINDA DİJİTALLEŞME

3.1 FinTek Kavramı ve Sermaye Piyasalarına Etkisi

İhtiyaç duyulan fonların etkin kullanımı faaliyetlerini kapsayan –finans- ve üretim amacıyla geliştirilen araçları ve bilgiyi kapsayan –teknoloji- kelimelerinin bir araya gelmesi ile ortaya çıkan finansal teknoloji (TCMB:2016), finansal sistem için önemi giderek artan kavramlar arasında yer almakta ve FinTek şirketleri finansal hizmetler endüstrinde yıkıcı güç olarak ortaya çıkmaktadır. FinTek kavramının genel kabul görmüş bir tanımı olmamakla birlikte**,** finansal hizmetler endüstrisini dönüştürme potansiyeline sahip çeşitli yeni teknolojiler ve finans alanındaki uygulamaları olarak tanımlanması mümkündür.

Bu teknolojiler, genellikle yerleşik bankalar ve aracılar gibi hizmet sunucuları tarafından sunulmakta olan finansal hizmetleri ayrıştırarak çoğunlukla internet kullanımıyla otomatikleştirilmiş biçimde sunmaktadır. Finansal teknoloji denkler arası borçlanma, kitle fonlaması, akıllı sözleşmeler, robo-tavsiye, sanal para ve dağıtılmış defter teknolojisi gibi finansal hizmetleri kapsamakta olup finansal hizmetlerde yaşanan inovasyon örneklerinden bazıları tablo 1'de gösterilmektedir.

Finansal Teknoloji Hizmetleri	
Tanım	**Açıklama**
Dağıtılmış Defter Teknoloji	Finansal aktörler arasındaki veri işleme ve paylaşma eylemlerini kolaylaştırmak için fikir birliği protokolleri ile her güncelleme hakkında mutabakat sağlanan dağıtılmış veri tabanı sistemidir. Bilgisayar biliminin ve kriptografinin çeşitli alanlarından kavramlar, bu sistemi gerçekleştirebilmek için kullanılır.
Denkler arası borçlanma	Kişiler veya firmalar arasında bir internet sitesi aracılığı ile fonlama yapılması yöntemidir.
Kitle Fonlaması	Fon arz edenler ile fon talep edenler arasında internet üzerinden bağlantı kurulmasını sağlamaktadır. Bu sistem ile gerçekleştirilmesi planlanan projeler için gereken maddi desteğin platformlar aracılığı ile toplanması mümkündür.
Akıllı Sözleşmeler	Kendiliğinden uygulayan, teyit eden ve sınırlayan bilgisayar protokolleri anlamına gelmektedir. Protokoller sayesinde varlıkların bir finansal sözleşmenin şartlarına bağlı olarak aracılar olmadan el değiştirmesi mümkün hale gelmektedir

Robo-Tavsiye	Algoritmalar aracılığı ile portföy dağılımını sağlayan ve otomatikleştirilmiş yatırım tavsiyelerinde bulunan uygulamalardır.
Bulut Teknolojisi	İnternet üzerinde barındırılan tüm uygulama, program ve veriler için sağlanan online depolama hizmetidir. İnternete bağlı olan her cihaz ile bu verilere erişim sağlanması mümkündür.
Sosyal Alım Satım Platformları	Bir sosyal ağ aracılığı ile işlemlerin takip edilmesi kopyalanması hizmetleri sunmaktadır.

Tablo 1

Dağıtılmış defter teknolojisi, makine öğrenimi ve yapay zeka gibi gelişmekte olan teknolojilerin, FinTek girişimcilerini ve geleneksel şirketleri desteklemek için kullanılma potansiyeline ek olarak finansal hizmetler sektörünü değiştirme potansiyeli de bulunmaktadır. Tablo 2'de, teknoloji trendlerine karşı haritalandırılan bazı inovasyon kullanım örnekleri gösterilmektedir.

Fırsat alanlarının teknoloji trendlerine haritalandırılması										
ALAN	**İŞLEV**	Bulut Teknolojisi	Süreç ve Hizmet Dışsallığı	Robotik Süreç Otomasyonu	İleri Analitik	Dijital Dönüşüm	Blok Zinciri	Akıllı Sözleşmeler	Yapay Zekâ	Nesnelerin İnterneti
Müşteri hizmetleri	Müşteri edinim	✓	✓	✓		✓	✓			
	Müşteri analitiği	✓			✓	✓				
	Araştırma	✓			✓				✓	✓
	Müşteri ilişkileri yönetimi	✓			✓	✓			✓	
	İhraç, birleşme ve satın alma	✓	✓	✓	✓	✓	✓			
İşlem	İşlem öncesi analiz	✓			✓	✓				
	İşlem gerçekleştirme	✓	✓		✓	✓			✓	✓
	İşlem sonrası analiz	✓	✓		✓	✓				
İş yönetimi	Maliyet Şeffaflığı	✓			✓					
	İş sürekliliği yönetimi	✓	✓			✓				
Veri yönetimi	Piyasa haberleri ve verileri	✓	✓		✓	✓				
	Referans verileri	✓	✓	✓	✓		✓			

İşlem sonrası süreç	Takas ve takas öncesi işlemler	✓	✓	✓			✓	✓		
	Teminat ve marjın yönetimi	✓	✓	✓			✓			
	Saklama hizmeti	✓	✓	✓			✓			
	Hazine işlemleri	✓	✓	✓	✓					
	Mutabakatlaşma	✓	✓	✓	✓		✓		✓	
	İşlem raporlama	✓	✓	✓	✓				✓	
	Ücretler ve faturalandırma	✓	✓	✓	✓					
	Vergi işlemleri	✓	✓	✓	✓		✓	✓	✓	
Risk kontrolü yönetimi	Kredi, piyasa ve likidite riski	✓	✓	✓	✓					
	Kurumsal risk yönetimi	✓			✓	✓			✓	
Mali kontrol	Sermaye yönetimi	✓	✓	✓	✓					
	Bağımsız fiyat doğrulama	✓		✓	✓					
	Ürün kontrolü	✓		✓	✓					
	Düzenleyici raporlama	✓		✓	✓					
Uyum	Düzenleyici tarama ve uyum	✓	✓		✓				✓	
	Kara para aklanmasının önlenmesi	✓	✓		✓				✓	
	Müşteriyi tanıma	✓	✓	✓	✓					
	Rüşvetle ve yolsuzlukla mücadele	✓	✓		✓					
	Çalışan ve piyasa kötüye kullanımı gözetimi	✓			✓				✓	
	Politika belirleme, izleme ve test	✓		✓	✓	✓				
Bilişim	Siber güvenlik	✓	✓		✓				✓	
	Kimlik ve erişim yönetimi	✓	✓				✓	✓	✓	
	BT hizmetleri	✓	✓	✓		✓			✓	
Hukuk		✓	✓	✓	✓	✓	✓	✓	✓	
İK		✓	✓	✓					✓	

Tablo 2 (Kaynak: Capital Markets: innovation and the FinTech landscape)

Son yıllarda FinTek blok zinciri teknolojisi, robo-tavsiye, P2P kredi, kitle fonlaması ve mobil ödeme üzerine yoğunlaşan önemli gelişmelerle birlikte dünya

genelinde yoğun ilgi görmektedir. Bu bağlamda, Şekil 3'de 2005-2016 yılları arasında FinTek şirketlerine yapılan küresel yatırımlar[2] gösterilmektedir.

Şekil 3 (Kaynak:KPMG Global analysis of investment in fintech)

Finansal sistemi çeşitli kanallardan etkileyen FinTek sayesinde finansal sistemin gelişmediği ülkelerde tabana yayılma artarken geleneksel kaynaklardan finansman sağlama imkânı bulamayan gerçek ve tüzel kişiler de yeni aracılardan[3] kaynak edinme imkânına kavuşabilmektedir. Diğer taraftan, bu durum FinTek şirketlerinin rekabeti artırarak maliyet avantajı sağlama ve etkinliği artırma potansiyeli olduğunu da göstermektedir.

Finansal sisteme yansımaları bulunan FinTek uluslararası kuruluşlar tarafından da yakından takip edilmektedir. Örneğin, FSB Başkanı'nın 30 Ağustos 2016 tarihinde G-20 liderlerine gönderdiği mektupta, FSB ve diğer standart belirleyici kuruluşlarca 2017 yılı başında FinTek vaka analizlerine yönelik bir çalışma hazırlanacağı ve düzenleme gerektirebilecek hususlara dikkat çekileceği belirtilmiştir (TCMB 2016).Benzer şekilde, IOSCO tarafından "research report on financial technologies" isimli bir rapor yayınlanmış olup söz konusu raporda borç verme ve kitle fonlaması platformları ile blok zinciri teknolojisinin menkul kıymet düzenleyicileri açısından öne çıktığı ifade edilmiştir.

3.2 FinTek'in Genel Zemini

FinTek'in yaygınlaşmasının temelinde; büyük veri kümelerinin analizini mümkün kılacak düzeyde bilgi işlem gücünün artması, dijitalleşme, malların ve

[2] Yatırımcıların global olarak yıkıcı iş modellerini satın almasından dolayı 2014 ve 2015 yıllarında FinTek'e büyük bir yatırım yapıldı. 2016 yılında ise jeopolitik ve makroekonomik belirsizliğin artmasıyla yatırımcıların inovatif çözümlerin ölçeklenebilirliği ve ticarileştirilebilirliği konusunda daha sınayıcı olmasından dolayı yatırımlarda düşüş yaşanmıştır.

[3] Kitle fonlaması, denkler arası borçlanma vb.

hizmetlerin daha geniş düzeyde erişilebilir hale gelmesi, aracıların ortadan kaldırılması ve düşük işlem maliyetleri olarak sayılabilecek ancak bunlarla sınırlı olmayan nedenler bulunmaktadır. Örneğin, bazı hizmetlerin fiziki hizmet yerleri olmaksızın internet ortamından sağlanması, menkul kıymetlerin kâğıt sertifikalar halinde ihraç edilmesinin ve saklanmasının bırakılıp kaydi sistemlere geçilmeye başlanılması gibi gelişmeler bir yandan sabit maliyetleri düşürürken diğer yandan da işlemlerin etkin bir şekilde gerçekleştirilmesini sağlamaktadır. Ayrıca, FinTek'in yaygınlaşabilmesinde rol oynayan diğer bir önemli faktör ise finansal düzenlemelerdir. Çünkü düzenlemeler nedeniyle aracılık faaliyetlerinde denkler arası borçlanma veya kitle fonlaması gibi alternatif yöntemlere bir miktar geçiş olması ve daha birçok inovatif iş modeli mümkün hale gelebilmektedir. Bu noktada ise FinTek'in nasıl düzenlenmesi gerektiği önem kazanmakta olup söz konusu husus bu çalışmanın 3.6'ncı bölümünde yer almaktadır.

3.3 Bilgi İşlem Gücünün Büyümesi

1965 yılında Intel'in kurucu ortağı Gordon Moore tarafından işlemci gücünün her 24 ayda bir iki katına çıkacağı öngörülmüştür. Bu doğrultuda günümüzde; işlemci gücünün maliyeti, yaklaşık olarak 1950'de başlayan bilgisayar çağının ilk 50 yılında 10 milyar kez azalmış, bellek kartlarının gücünde son 10 yılda bin kat artış olmuş, dizüstü bilgisayarlar 30 yıl önceden 100 bin kat fazla olan 1 terabayt boyunda depolama yapabilir hale gelmiş ve tek bir akıllı telefon NASA'nın 1969'da sahip olduğu bilgi işlem gücünden daha fazlasına sahip olmuştur.(Richard &Daniel Susskind 2016)

Bilgi işlem gücünün artması; verilerin toplanması, işlenmesi ve depolanmasının maliyetinin düşmesi, erişilebilir veri ve veri kaynaklarının üssel olarak artması, verilerin paylaşılabileceği ve uygulamaların geliştirilebileceği altyapı ve platformların oluşması gibi faktörler yukarıda Tablo-1'de gösterilen FinTek kategorilerinin ortaya çıkmasına ve büyümesine katkıda bulunuyor. Bu sayede de artık ihraççılar, yatırımcılar ve aracılar, geçmişten çok farklı yollarla iletişim kuruyor, araştırma yapıyor, sosyalleşiyor, paylaşıyor, işbirliği yapıyor, rekabet ediyor, ticaret yapıyor ve böylece de düzenleyici paradigmaya[4] meydan okuyor. Örneğin, günümüzde yukarıda açıklanan kapsamda teknolojide meydana gelen gelişmeler sayesinde yatırımcılar; sosyal alım satım platformlarında ve melek yatırımcı sitelerinde diğer yatırımcıları takip edebilir, mevcut piyasa verisi sayesinde yapay zekâ ve sosyal medya analizleri ile de menkul kıymet alım satımı ve yatırım kararı verme konularında analiz yapabilir konuma gelmiştir. Ayrıca kitle fonlaması platformları internet ortamında projelere katılımcı finansman desteği sağlanmasına aracılık etmekte, denkler arası borçlanma platformları kredi satmakta veya satılmasına aracılık etmekte, robot-tavsiye uygulamaları otomatikleştirilmiş yatırım tavsiyeleri sunmakta ve sosyal alım-satım platformları bir sosyal ağ aracılığı ile yatırım hizmetleri sunmaktadır.

[4] FinTek'lerin düzenlemesi konusu bu çalışmanın 3.6'ncı bölümünde incelenmiştir.

3.4 Geniş Kapsamlı Erişilebilirlik ve Hizmetlerin Maliyetinin Düşmesi

Küresel bağlantı ile ürün ve hizmetlere daha geniş tabanlı erişimi kolaylaştıran internet, mal ve hizmetlerin maliyetinin düşmesini hatta bazı durumlarda ortadan kalkmasını sağlamıştır. FinTek ise bu eğilimin bir tezahürüdür. Öyle ki teknoloji kullanımı ile,

- Kitle fonlaması platformları, daha önceleri yüksek gelirli yatırımcılara ayrılan sermaye yatırımlarına bireysel yatırımcıların da erişmesini,

- Robo-tavsiye uygulamaları daha önce kurumsal ve özel bankacılık müşterileri için mümkün olan modern portföy teorisine dayalı yatırımları bireysel yatırımcıların da gerçekleştirmesini,

- Belirli sosyal alım satım platformları ise sıfır komisyon ile işlemlerin yapılabilmesini

mümkün hale getirmiştir.

3.5 Aracıların Ortadan Kaldırılması

Yukarıda açıklananlarla yakından ilişkili olarak teknoloji ve internet kullanımının yaygınlaşmasıyla aracıların ortadan kalkarak yerini teknolojik çözümlerin alması gündeme gelmektedir. Örneğin, Tripadvisor seyahat acentelerini, Amazon kitapevlerini, AirBnb ve Tujia otelleri, Uber ve Didi Dache ise lisanslı taksileri devre dışı bırakma yolunda ilerlemektedir. Benzer şekilde blok zinciri, robo-tavsiye uygulamaları ve kitle fonlaması platformları gibi inovatif FinTek iş modelleri ise düzenlenmiş bazı faaliyetlerde aracıların ortadan kalkmasına yol açma potansiyeline sahiptir. Öyle ki kitle fonlaması platformları borsaların, otomatik yatırım tavsiyeleri sunan robo-tavsiye platformları geleneksel danışmanların, kredi veren veya verilmesine aracılık eden uçtan uça borç verme platformları ise bankaların aracılık rollerine talip olmaktadır. Bu durum da, günümüzde ayakta kalmak ve gelişmek isteyen finansal piyasa aktörleri için inovasyonun artık bir seçenekten ziyade zorunluluk olduğunu göstermektedir. Yani mevcut aktörlerin uzun vadede işlerini sürdürebilmeleri için oyunu değiştirmeleri gerekiyor. Bu nedenle, mevcut aktörlerin yıkıcı inovasyon ile pazar payını kaybetmek arasında bir seçim yapması gerektiği söylenebilir.

3.6 Regülatörlerin FinTek Yaklaşımı

Teknoloji dünyasında meydana gelen gelişmeler hayatın birçok alanını olduğu gibi finansal hizmetler endüstrisini de etkilemekte ve yeniden şekillenmesine neden olmaktadır. Finansal hizmetler endüstrisindeki bu yeniden şekillenmenin temelini ise genel olarak, mobil telefonların ortaya çıkışı, internet kullanımının yaygınlaşması, bilgi işlem gücünün artması, kriptografideki ilerlemeler, makine öğrenimindeki yenilikler gibi gelişmeler oluşturmaktadır. Teknoloji ile birlikte devam eden bu hızlı değişim bir yandan da FinTek sektörünün her geçen gün büyümesine ve finansal hizmetler endüstrisini dönüştürme potansiyelinin artmasına katkı sağlamaktadır. Bu

durumda da inovasyonun ve finansal hizmetler endüstrisinin geleceği için etkili regülasyonlara olan ihtiyaç artmakta ve regülatörler açısından FinTek'lere zarar vermeden, ancak aynı zamanda finansal sistemi güvence altına alarak FinTek sektörünün nasıl düzenlenebileceği hususu önemli olmaktadır. Çünkü FinTek regülasyonu, değişen finansal hizmetler dünyasında tutarlı bir manzara oluşturabilmenin temel taşıdır. Ayrıca FinTek regülasyonunun, özellikle geleneksel olmayan finansal hizmet şirketlerinin sisteme girişi için kolaylık sağlama veya engel olma potansiyeli olduğundan iki tarafı keskin kılıca benzetilmesi mümkün olup regülasyonların bu çerçevede yapılması gerekmektedir.

Bu noktada uluslararası alanda Singapur, Avusturya ve İngiltere yatırımcının korunması hususundaki hassasiyeti devam ettirirken FinTek inovasyonlarının gelişmesi amacıyla regülasyonlarını geliştirme konusunda öne çıkmaktadır. FinTek regülasyonlarının herkese nasıl fayda sağlayacağına dair önemli örneklerinden biri ise Singapur'dur. Ülke, yeni yerli şirketlerin minimum bürokratik işlemle pazarda test ve dağıtıma başlayabilmesi konusunda sağlanan regülasyon esnekliği sayesinde FinTek inovasyonunun merkezlerinden biri olmuştur. Ancak hemen belirmek gerekir ki Singapur, Silikon Vadisi ve Londra gibi diğer FinTek merkezleriyle karşılaştırıldığında şirketlerin sermayeye erişimi açısından hala geride kalmaktadır. Bununla beraber, Singapur Merkez Bankası tarafından FinTek projelerine beş yıl için 167 milyon dolar yatırım yapılması taahhüt edilmiştir. Ayrıca, hükümet tarafından İngiltere ile FinTek şirketlerinin FCA ve Singapur'daki mukabiline başvurmasını karşılıklı olarak kolaylaştıran "FinTek Köprüsü" başlıklı ortaklık imzalanmıştır. Bu ortaklık, FinTek şirketlerinin düzenleyici kısıtlamalar olmaksızın iki ülke arasında ölçeklenmesini sağlanmaktadır. Diğer taraftan, Dünya çapında bir çok fon ve kaynaktan oluşan regülatör kurum bulunmaktadır. Ancak finansal istikrar ve yatırımcının korunması gibi geleneksel yükümlülüklerin yerine getirilmesinin yanı sıra inovasyonun teşvik edilmesi için finansal regülatörünün yönetimine yetki veren tek ülke İngiltere'dir. İngiltere uluslararası alanda inovasyonu ilerletmek ve ülkeler arasındaki işbirliğini teşvik etmek için Singapur örneğine benzer bir işbirliğini Avustralya ile de yapmaktadır. Bu ortaklıklar, İngiltere'nin FinTek regülasyonlarına yönelik çözüm geliştirmeye yardımcı olmak için devam etmekte olan stratejilerinin küçük bir örneğidir. Ayrıca İngiltere'de FCA tarafından, FinTek şirketlerine düzenlemelerin kısıtlamaları olmaksızın yeni bir fikri deneme imkânı sağlama amacı ile "sanal ortam" uygulaması gerçekleştirilmektedir ve uluslararası piyasalarda görüldüğü üzere bu "sanal ortam" uygulamaları ayrıca ülkelerin FinTek öğrenme hızını artırmaya da yardımcı olmaktadır.

Esas itibariyle İngiltere'de iki sebeple regülasyon esnekliği teşvik edilmektedir. Bu sebeplerden ilki, FinTek'lerin büyük finansal kuruluşlar için hazırlanmış olan regülasyonlara uymasını beklemenin onların sisteme girişi için engel oluşturabilecek olması, ikincisi ise mevcut şirketlerin yanı sıra FinTek şirketleriyle olan işbirliği ve koordinasyonun geliştirilmesinin regülatörlere de düzenleme yapma konusunda yararlı olmasıdır.

Avustralya'da ise FinTek şirketlerinin lisanslanması ve izlenmesi gibi hususlarda düzenleme yapma konusunda ASIC görevlendirilmiştir. ASIC tarafından, bu görev hem yatırımcıların hem de şirketlerin sisteme katılımının sağlanması amacıyla, sistemde rekabetin artırılması ve yeni modellere güvenin sağlanması gereksinimleri dikkate alınarak yerine getirilmektedir. Bu amaca yardımcı olması için ASIC tarafından, FinTek şirketlerinin regülatör onayı alarak düzenlenen sisteme girişini kolaylaştıran ve giriş için tek nokta olan "İnovasyon Merkezi" geliştirilmiştir.

İngiltere, Singapur ve Avusturalya gibi uluslararası örnekler FinTek regülasyonlarının FinTek'lere zarar vermeden, ancak aynı zamanda finansal sistemi güvence altına alarak yapılması gerektiğini göstermektedir ki bu da FinTek şirketlerine inovasyonları uygulamak için özgürlük ve esneklik kazandıran aynı zamanda yatırımcı güvenini sağlayan bir ortam oluşturulması gerektiği anlamına gelmektedir.

Bu bağlamda, regülatörlerin FinTek'lere[5] yaklaşımının temel özellikleri aşağıda belirtilmektedir:

- FinTek şirketleri için inovasyonu sağlayacak "sanal ortam" yaratılması.
- Düzenleyici kurumlar ve yurtdışı muhatapları arasında ortaklık kurulması.
- Düzenleyici kurumlar ve FinTek liderleri arasında inovasyon konusundaki problemleri ve bunların çözümlerini belirlemek için uyumun sağlanması.
- FinTek inovasyonlarının büyümesini sürdürmek, rekabeti korumak ve sonuçta tüketicilere fayda sağlamak için FinTek'lere yönelik devlet desteğinin artırılması.

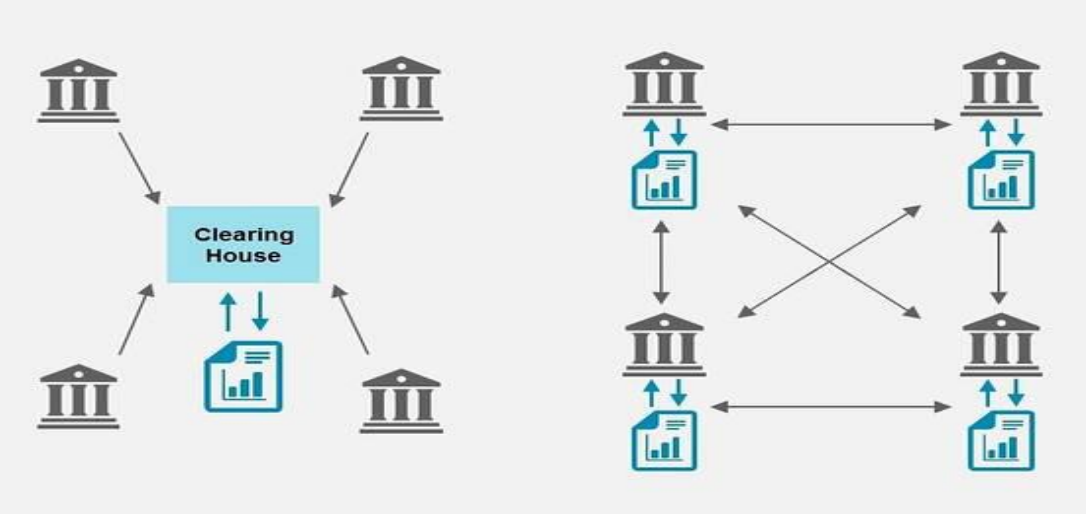
[5] Regülatörler açısından en önemli zorluklardan birisi FinTek şirketlerinin nasıl sınıflandırılacağı konusudur.

4. DAĞITILMIŞ DEFTER TEKNOLOJİSİ VE ÖZELLİKLERİ

Yukarıda açıklanan FinTek kategorilerinden sermaye piyasalarında önemli derecede yıkıcı etki yaratma potansiyeline sahip olma hususunda blok zinciri/DLT öne çıkmaktadır. Bu bağlamda çalışmanın bu bölümünde ve genel olarak sonraki bölümlerinde dağıtılmış defter teknolojisi ve özelliklerine odaklanmaktadır.

Sermaye piyasaları, veri paylaşımı gibi süreçlerden dolayı yapısal olarak birbiri ile etkileşime girme ihtiyacı olan çeşitli aktörlerden oluşmaktadır. Varlık sahipliği kayıtlarının tutulması için aktörlere özel ve diğer aktörlerle paylaşılmayan veri tabanı sisteminin kullanılması ise bu ihtiyacı karşılamaya yönelik teknik altyapının büyük ölçüde entegre olmamasına neden olmaktadır. Avrupa Merkez Bankası tarafından 2016 yılında yayınlanan *"Distributed ledger technologies in securities post-trading"* isimli raporda bu ayrık sistemin uluslararası menkul kıymet işlemlerinin yüksek maliyetlerinden dolayı Avrupalı yatırımcılar arasında risk paylaşımı potansiyelini sınırladığına, ayrıca operasyonel riskin artmasına sebep olduğuna yönelik yorum yapılmıştır.

Disributed Ledger Technologies (DLTs) finansal aktörler arasındaki veri işleme ve paylaşma eylemlerini kolaylaştırmak için bir yöntem önermekte ve son birkaç yıldır hem özel şirketlerin hem de devlet kurumlarının yoğun ilgisini çekmektedir (Accenture 2015). Şekil 4'de örnek olarak bankalar konsorsiyumu tarafından bir aracı olmadan doğrudan birbirleriyle işlemlerin takasını gerçekleştirmek için DLT'lerin nasıl kullanılabileceği gösterilmektedir. Merkezi bir saklama kuruluşundan sorgulama yapmak yerine her banka varlık sahipliği kayıtlarının lokal kopyasını tutar ve bu kayıtların senkronizasyonu DLT kullanılması ile sağlanır. Bu şekildeki veri paylaşımı iki taraflı olarak, diğer bir deyişle doğrudan iki taraf arasında yapılabilir.



Şekil 4: Solda: Takas kurumu gibi merkezi bir otoritenin varlık sahipliği kayıtlarını tuttuğu mevcut sistem. Sağda: DLT kullanımı ile senkronize olması sağlanan varlık sahipliği kayıtlarının her bir bankada kopyasının tutulduğu sistem.

DLT kavramı ilk olarak 2009 yılında, takma adıyla Nakamoto tarafından dijital para birimi Bitcoin ile finans dünyasının gündemine getirilmiştir(Nakamota 2009). Nakamota, tamamıyla dağıtılmış dijital para sisteminin gerçekleştirilmesinde başlıca engel olan çifte harcama sorununa yeni bir çözüm önermişti. Bitcoin'in kullanıma sunulmasından bu yana DLT'lerin uygulama alanları, dağıtılmış oylama sistemlerinden gayrimenkul ve resim gibi gerçek hayat varlıklarının mülkiyetinin takip edilmesine kadar yeni alanlara yayılmıştır. Bu çalışmada ise, DLT'lerin teknik anlamda incelenmesi ile Türkiye sermaye piyasalarının finansal yapısında sunabileceği imkânlara odaklanılmıştır.

4.1 Genel Kapsamlı Teknik Açıklama

Esas itibarıyla DLT, kullanıcıların fikir birliği protokolleri ile her güncelleme hakkında mutabakat sağladığı dağıtılmış veri tabanı sistemi olarak ifade edilebilir. Çalışmanın ilerleyen bölümlerinde incelenen bilgisayar biliminin ve kriptografinin çeşitli alanlarından kavramlar, bu sistemi gerçekleştirebilmek için kullanılır.

Genel bir DLT protokolünde, dağıtılmış bir veritabanı olarak neredeyse değiştirilemez bir blok zinciri oluşturulabilmesi için blok denilen veri kümelerinin birbirine nasıl bağlanması ve sistemdeki kullanıcılar arasında nasıl dağıtılması gerektiği belirtilir. Her blok, veritabanının blok oluşturulduğu andaki durumunu temsil eder ki bu da veritabınının tüm geçmiş durumlarının korunması anlamına gelmektedir. Veri güncelleme işlemi ise blok zincirinin sonuna yeni bir blok eklenmesi suretiyle gerçekleştirilmektedir.

DLT sisteminde, her kullanıcı blok zincirinin yerel bir kopyasını tutar, bu da tüm kullanıcıların bir sonraki bloğa hangi işlemlerin dâhil edileceğine mutabık olmaları için fikir birliği protokolünün varlığını gerektirir. Fikir birliği protokolünün, DLT kullanılan uygulamanın amacına bağlı olarak farklı şekillerde tasarlanabilmesi mümkündür. Fikir birliği protokolü bölüm 4.8'de daha ayrıntılı bir şekilde incelenmiştir.

Blok zincirindeki her blok, blok verisinin elektronik imzası olarak da ifade edilebilecek eşsiz bir özet değeri[6] tanımlayıcısına sahiptir. Blokları birbirine bağlamak için her blok, üst bloğun eşsiz özet değeri tanımlayıcısını kullanarak üst bloğu referanslar. Bu referanslama ile oluşan bağlantılar, genellikle başlangıç bloğu olarak adlandırılan blok zincirinin ilk bloğuna[7] kadar uzanan bir zincir oluşturur. Blok verisinde üst bloğun özet değeri bulunduğu için bloğun özet değeri de üst bloğunun özet değerine bağlı olacaktır. Böylece, herhangi bir blokta saklanan veride yapılan değişiklik bloğun kendi özet değerinin ve o bloğa bağlı azalan blokların özet değerinin değişmesine neden olacaktır; yani blok zincirinde saklanan bir bloğun verisini

[6] Temel kriptografik terimlerden biri olan "özetleme fonksiyonu", değişik uzunluktaki bit dizilerini sabit uzunluktaki bit dizilerine taşıyan polinomsal zamanda kolay hesaplanabilen fonksiyondur. Görüntü kümesindeki sabit uzunluklu oluşan bu bit dizisine ise "özet değer" (hash value) adı verilir.

[7] Genesis blok olarak da adlandırılmaktadır.

değiştirmek için bloğa bağlı tüm azalan blokların, zincirin geçerli kabul edilebilmesini sağlamak adına yeniden hesaplanması gerekir. Kullanıcının yeni bir bloğu hesaplaması ve sisteme yayınlaması için seçilen prosedüre bağlı olarak bu özellik yeteri kadar azalan bloğa sahip olunduktan sonra blok zincirindeki verileri değiştirmeyi neredeyse imkânsız hale getirebilir (Andreas 2014).

Blok içerisindeki verilerin, blok zincirini kullanılan uygulamanın amacına bağlı olarak farklı şekillerde yapılandırılabilmesi mümkünse de genel olarak üst bloğun oluşturulduğu an ile bir sonraki bloğun oluşturulması arasındaki zaman diliminde doğrulanan işlemlerin listesi, bu işlem listesinin özet değeri ile birlikte tutulur. İşlem listesinin özet değeri ise merkle ağacı algoritması kullanılarak elde edilir. Merkle ağacı algoritması bölüm 4.4'de daha ayrıntılı bir şekilde incelenmiştir.

Bir hesabın sahibinin, o hesaptaki varlıklara ilişkin işlemleri gerçekleştirebilecek tek kişi olmasını sağlamak için açık anahtarlı şifreleme yöntemi kullanılır. Sistemde yer alan her hesap açık bir anahtarla ilişkilendirilir. Varlık transferi işleminin gerçekleştirilebilmesi içinse bu açık anahtara karşılık gelen özel anahtarla oluşturulan dijital imzanın işleme dâhil edilmesi gerekir. Bu durumda yalnızca hesabın sahibinin özel anahtara erişimi olduğu varsayılırsa hesaptaki varlıkların bu yöntemle hırsızlıktan korunduğu söylenilebilir. Açık anahtarlı şifreleme yöntemi bölüm 4.3'de daha ayrıntılı bir şekilde incelenmiştir.

4.2 Özetleme Fonksiyonları

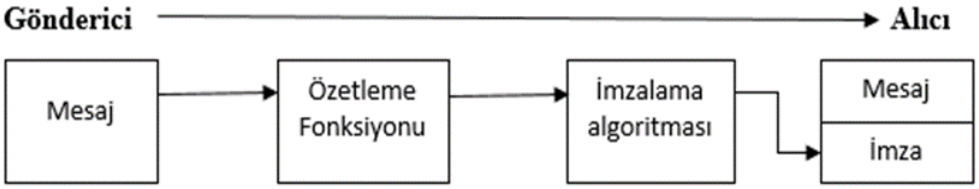
Blok zinciri uygulamalarında sistemin güvenliğinin sağlanması, kimlik doğrulama ve veri şifreleme gibi çeşitli işlemlerin gerçekleştirilmesi amaçlarıyla kriptografi yöntemleri kullanmaktadır. Bu nedenle blok zinciri sistemlerinin yeteneklerinin ve kısıtlamalarının tam olarak anlaşılabilmesi için kriptografik yöntemlerden olan "özetleme fonksiyonu" ile "açık anahtarlı şifreleme" nin nasıl çalıştığının incelenmesi gerekmektedir. Bu bölümde de blok zinciri uygulamalarında bahse konu amaçları sağlamak için kullanılan kriptografik sistemler açıklanmaktadır.

Temel kriptografik terimlerden biri olan "özetleme fonksiyonu" veya diğer adıyla tek yönlü özetleme fonksiyonu[8], değişik uzunluktaki bit dizilerini sabit uzunluktaki bit dizilerine taşıyan polinomsal zamanda kolay hesaplanabilen fonksiyondur. Görüntü kümesindeki sabit uzunluklu oluşan bu bit dizisine ise "özet değer"[9] adı verilir

Özetleme fonksiyonları değişken m uzunluklu mesajların sabit n uzunluklu mesajlara indirgenmesi amacıyla kullanılır(m>n).Seçilen h özetleme fonksiyonunun iyi olarak nitelendirilebilmesi için fonksiyon iki farklı m1 ve m2 mesajlarını aynı özet değerine taşımamalı ve verilen bir y özet değerinden m mesajı polinomsal zamanda hesaplanamamalıdır (William 2011).

[8] one-way hash function
[9] hash value

Özetleme fonksiyonlarının kullanımı daha çok sayısal imza ve veri bütünlüğünün korunması alanlarında yaygındır. Örneğin sayısal imza uygulamalarında uzun mesajlar ilk olarak bilinen bir özetleme fonksiyonu ile sabit uzunluklu kısa bir diziye özetlenir ve bu özet değer imzalanır.



Şekil 5: Şifrelenmemiş bir mesajın bütünlüğünün ve doğruluğunun korunması için özetlenip imzalanması.

Özetleme fonksiyonu bilginin bütünlüğünü sağlamak için de kullanılabilmektedir. Fonksiyonun tanım kümesindeki her mesajı görüntü kümesinde farklı bir özet değerine taşıması gerektiği düşünülürse içeriği değiştirilmiş bir mesajın özet değeri de farklı çıkacaktır. Dolayısıyla mesajı alan kişi mesajı kendisinin de bildiği özetleme fonksiyonundan geçirecek ve elde ettiği özet değerle kendisine gönderilen özet değeri karşılaştıracaktır. Mesajın bütünlüğünün korunduğunun ispatı için bu iki değerin uyuşması gerekmektedir. Ayrıca, özet değeri veri kümelerinin birbirine bağlanılarak özet zinciri oluşturulması amacıyla da kullanılmaktadır. Özet zinciri oluşturmak için, her veri kümesi bir önceki veri kümesinin özet değerini kullanarak bir önceki veri kümesini referanslar ve bir önceki veri kümesinin özet değeri mevcut veri kümesinin özet değerinin oluşturulmasında da kullanılır. Bu durumda mevcut veri kümesinin özet değeri önceki veri kümesinin özet değerine bağlı olur. Böylece önceki veri kümelerinde yapılan değişiklikler dolayısıyla sonraki veri kümelerinin de özet değişecektir ki bu durumda da doğrulama hatası almamak için veri kümesine bağlı tüm azalan veri kümelerinin yeniden hesaplanması gerekir. Blok zinciri uygulamalarında genellikle özet değerleri bu amaçla kullanılmaktadır.

Özetleme fonksiyonları yukarıda da bahsedildiği gibi herkesçe bilinebilen ve gizli anahtarı olmayan tek yönlü fonksiyon uygulamalarıdır. Eğer belli bir mesajın değiştirilip değiştirilmediğini tespit etmeye yönelik kullanılırlarsa "değişiklik tespit kodları"[10]adını alırlar. Bu alanla ilgili olarak gizli bir anahtar içeren ve veri bütünlüğünün yanı sıra veri kaynağının doğrulanması işleminde de kullanılan özetleme fonksiyonlarına ise "mesaj doğrulama kodları"[11] adı verilir.

Özetleme fonksiyonunun amacı, bir dosya, mesaj veya diğer bir veri bloğunun parmak izini üretmektir. Güvenli özetleme fonksiyonlarının özellikleri aşağıda verilmekte olup esas olarak iki mesaj için aynı özet değerini bulmak çok zor olmalı ve özet açık bir şekilde mesajla ilişkili olmamalıdır[12] (William 2011).

[10] Detection Codes
[11] Message Authentication Codes
[12] Mesajın karmaşık doğrusal olmayan bir fonksiyonu olmalıdır.

- H herhangi boyutlu bir M mesajına uygulanabilir.
- H sabit uzunluklu bit çıkış((h) üretir.
- H(M), verilen bir M mesajı için kolay üretilebilir.
- Verilen bir h değeri için, H(x)=h'yı sağlayan x'i bulmak hesaplama bakımından verimsizdir. Bu H(x)'in tek yönlü özelliğidir.
- Verilen bir x bloğu için H(y)=H(x) olan y!=x gibi bir y değerini bulmak hesaplama bakımından verimsizdir.[13]
- H(y)=H(x) için, bir (x,y) çifti bulmak hesaplama bakımından verimsizdir.[14]

Bugün sıklıkla kullanılan özetleme fonksiyonlarına örnek olarak 1992'de Ron Rivest tarafından geliştirilmiş MD5 (message-digest algorithm) algoritması gösterilebilir. NIST ve NSA'nın ortaklaşa geliştirmiş olduğu SHA(secure hash algorithm) ise yine NIST'ın özetleme fonksiyonları için belirlediği standart olan SHS (secure hash standart) içerisinde yer almış ve kullanımı yaygın olan bir özetleme algoritmasıdır.

4.3 Açık Anahtarlı (asimetrik) Şifreleme Sistemi

Blok zinciri ağında, doğrulama ve imzalama vasıtasıyla güvenli bir şekilde iletişim kurmak, kimlik doğrulamasını sağlamak ve işlemleri gerçekleştirmek için asimetrik şifreleme olarak da adlandırılan açık anahtarlı şifreleme sistemi kullanılmaktadır.

Açık anahtarlı sistemlerin kullanımı üzerine ilk öneri, 1976 yılında Diffie ve Hellman tarafından yapılmıştır (Hellman 1976). Ardından 1977 yılında Rivest, Shamir ve Adleman RSA kripto sistemi adlı yeni bir açık anahtarlı yöntemi bulmuşlardır (Rives,Shamir&Adleman 1978).

Geleneksel asimetrik olmayan gizli anahtarlı şifreleme yönteminde mesajın göndericisi ve alıcının birlikte paylaştığı tek bir anahtar kullanır ve bu anahtarın açıklanması durumunda haberleşme tehlikeye düşer. Açık anahtarlı şifreleme sistemi ise iki anahtar kullanımını gerektirir:

- Mesajları şifrelemekte ve imzaları doğrulamakta kullanılan herkes tarafından bilinen bir açık anahtar[15]
- Mesajları deşifrelemekte ve imza oluşturmakta kullanılan sadece alıcı tarafından bilinen bir gizli anahtar.

Temelde açık anahtarlı şifreleme sistemlerinin amacı belli bir anahtar üzerinde anlaşmanın ve karşı tarafa bu anahtarı güvenli bir şekilde ulaştırabilmenin zorluğunu

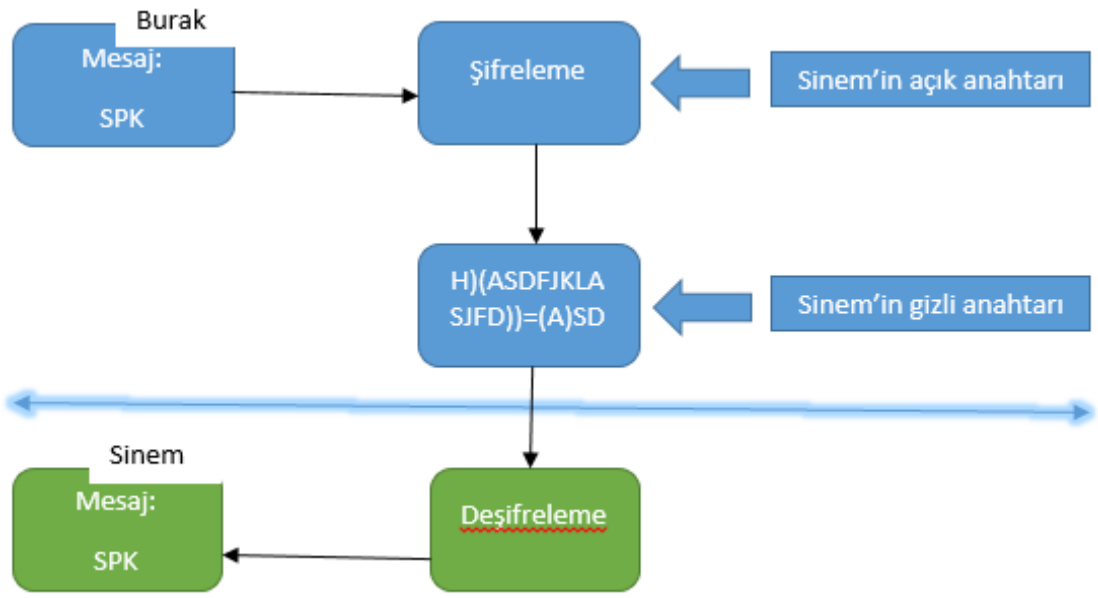
[13] weak collision resistance

[14] strong collision resistance

[15] Açık anahtar gizli anahtardan ve şifreleme hakkındaki diğer bilgilerden kolaylıkla hesaplanabilir. Bununla beraber açık anahtarın ve şifrelemenin bilinmesi, gizli anahtarı hesaplamak için hala hesaplama bakımından verimsizdir. Böylece açık anahtar, kendisi ile güvenli haberleşmek isteyen herhangi birisine dağıtılabilir.

ortadan kaldırmaktır. Açık anahtarlı şifreleme sisteminde tek yönlü bir mesajlaşma söz konusudur. Mesaj alıcısı sadece kendisinin bileceği "gizli anahtar" ve diğer kişilere dağıtabileceği bir "açık anahtar"dan oluşan anahtar çifti belirler. Kullanılan anahtar üretim algoritmasına göre bu iki anahtar arasında matematiksel bir bağlantı mutlaka olacaktır ancak bilinen açık anahtardan gizli anahtarın hesaplanmasının polinomsal zamanda imkânsız olması gerekmektedir.[16]

Mesaj göndericisi alıcıya ait herkesçe bilinen açık anahtarı kullanarak açık anahtarlı şifreleme algoritmasıyla göndereceği mesajı kapatır ve alıcıya gönderir, mesajın alıcısı ise yalnız kendisinin bildiği gizli anahtar ile deşifreleme algoritmasını kullanarak mesajı açabilir. Gizli anahtar yalnız alıcı tarafından bilindiği için başka birinin bu mesajı açması mümkün olmayacaktır.



Şekil 6: Açık anahtarlı şifreleme

Açık anahtarlı şifreleme sistemi mesaj içeriğini şifreleme işlemine benzer şekilde mesajı kimin ürettiğini doğrulama amacıyla sayısal imza uygulamalarında da kullanılmaktadır. Sayısal imza uygulamalarında, veriyi gönderen taraf kendisine ait gizli anahtar ile veriyi imzalar ve verinin alıcısı ise, göndericinin açık anahtarını kullanarak imzayı doğrular. Görüldüğü üzere mesaj içeriğinin şifrelenmesi işleminin tersine gizli anahtar veriyi imzalamakta kullanılırken açık anahtar ise imza doğrulamakta kullanılmaktadır. Uygulamada, sayısal imza kullanılırken depolama amaçları gözetilerek mesajın tamamı yerine özetleme fonksiyonu aracılığı ile üretilen özet değeri imzalanır. Örneğin Bitcoin'de işlem verilerinin kendisi değil sadece işlem verilerin özet değeri imza olarak kullanılacak şekilde şifrelenir. Bu sistemde

[16] Gizli anahtarın açık anahtardan polinomsal zamanda türetilmesini imkansız kılmak için Diffie ve Hellman'ın "tek yönlü fonksiyon" mantığı üzerine kurulu anahtar değişim protokolü (Key Exchange Method) vardır.

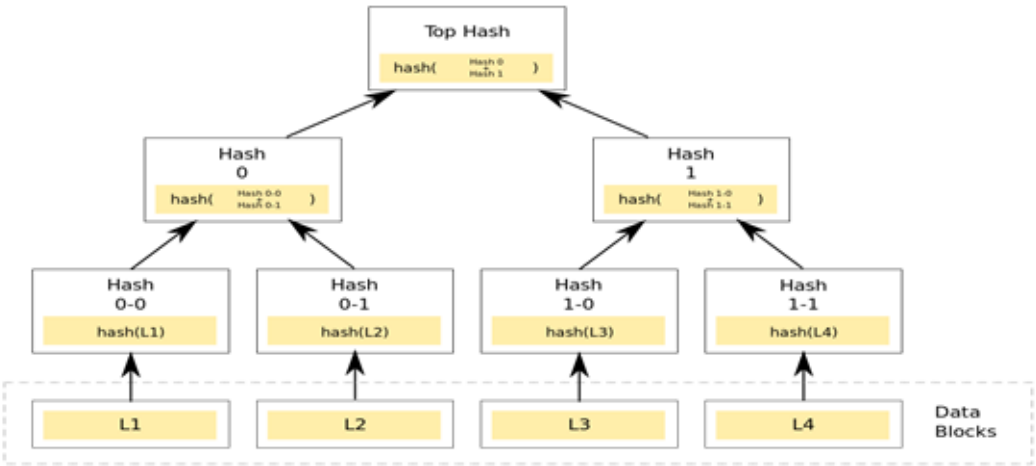
şifrelenmiş/imzalanmış mesaja erişimi olan herkesin göndericinin açık anahtarını kullanarak mesaj içeriğine ulaşabilecek durumda olmasından dolayı mesaj gizli değildir.

Birçok anahtar üretim algoritması olmasına rağmen Bitcoin de dâhil olmak üzere blok zinciri uygulamalarının çoğu gizli ve açık anahtarları oluşturmak ile verileri şifrelemek/imzalamak için eliptik eğri algoritmasını[17] kullanmaktadır. Bu algoritma doğru uygulandığı takdirde güvenlik ve hız bakımından eski anahtar üretme ve imzalama yöntemlerine kıyasla fayda sağlamaktadır. Bu çalışmanın kapsamı için, bu algoritmaların Hellman ve Daffie tarafından önerilen şartları yerine getirdiğine dikkat etmek yeterlidir.

4.4 Merkle Ağacı

Aynı zamanda ikili özet ağacı olarak da bilinen merkle ağacı, büyük veri kümelerini verimli bir şekilde özetlemek ve bu veri kümelerinin bütünlüğünü doğrulamak için kullanılan bir veri yapısıdır. Merkle ağacı blok zinciri uygulamalarında ise tüm işlemlerin bir blokta özetlenmesi, tüm işlemlerin dijital parmak izinin üretilmesi ve bir işlemin bloğa dâhil olup olmadığının doğrulanması konusunda verimli bir süreç sağlaması amaçlarıyla kullanılmaktadır.

Merkle ağacı, yaprak düğümler[18] hariç olmak üzere her düğümün, çocuk düğümlerinin şifreli özet değeri olduğu ikili ağaç[19] veri yapısıdır. Bu yapı, merkle kökü (kök düğüm) olarak adlandırılan en üstteki özet değerinin ağaçtaki tüm düğümlerin fonksiyonu olmasına yol açar. Böylece en üstteki özet değeri kullanılarak tüm veri yapısı etkin bir şekilde doğrulanabilir. Şekil 7'de 4 tane yaprak düğümü olan merkle ağacını gösterilmektedir.



Şekil 7: Merkle Ağacı

[17] Elliptic Curve Digital Signature Algorithm (ECDSA)

[18] Herhangi bir çocuk düğümü olmayan düğümleri ifade etmektedir.

[19] Ağaç terimi bilgisayar biliminde dallanan veri yapılarını tanımlamak için kullanılır ancak bu ağaçlar genellikle diyagramın en üstünde kök ve en altında yapraklar olacak şekilde başaşağı görüntülenir.

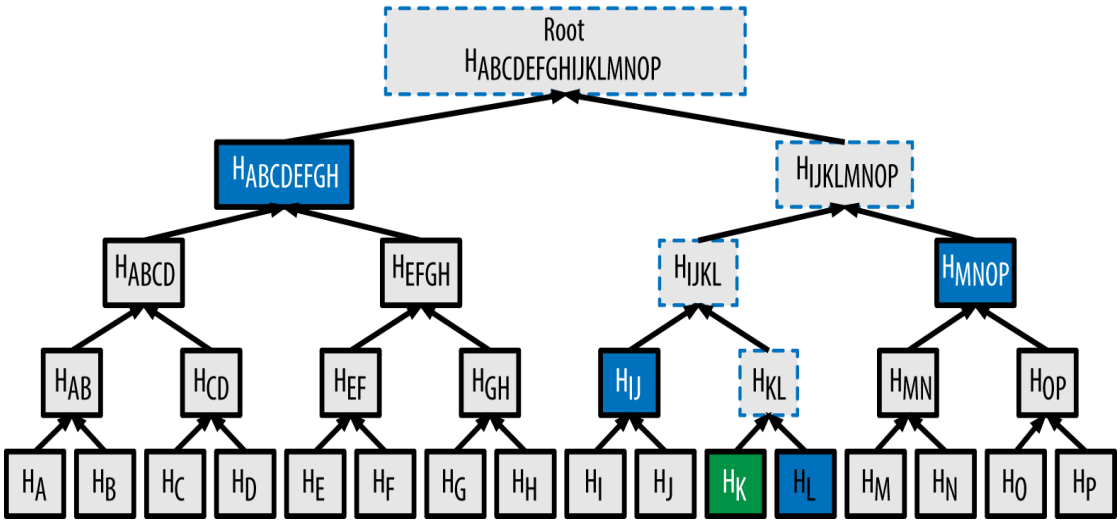
Merkle ağacı , merkle kökü olarak adlandırılan tek bir özet değeri elde edilene kadar düğüm çiftlerinin yinelemeli olarak özet değerinin hesaplanmasıyla aşağıdan yukarıya doğru oluşturulur (Ralph 1988). Şekil 7'deki örnekte, L1, L2,L3 ve L4 işlemlerine ilişkin verilerin doğrudan merkle ağacında saklanmasının yerine işlem verilerin özet değerleri elde edilerek her birinin yaprak düğümlerde saklandığı, daha sonra yaprak düğümlerin ardışık çiftlerinin özet değerlerinin birleştirilerek yaprak düğümü çiftlerine ilişkin yeni bir özet değerinin elde edilip bu değerin bir ana düğümde saklandığı ve bu işlemin üstte yalnızca merkle kökü olarak bilinen bir düğüm kalana kadar devam ettiği gösterilmektedir. Yani Şekil 7'de dört blok veriden, merkle ağacı kullanılarak bir özet değeri elde edilir. Yaprak olmayan düğümlerin her biri ise, bitişik iki çocuk düğümünün özet değeridir. Dört işlemden bir ağacın oluşturulması için kullanılan bu yöntem her hangi bir boyuttaki ağaçları oluşturmak için genelleştirilebilir. Örneğin, Bitcoin'de, binlerce işlem yukarda açıklanan yöntemle özetlenerek merkle kökü elde edilmesi suretiyle tek bir blokta saklanır. Blokta ister bir işlem isterse yüz bin işlem olsun merkle kökü her zaman sabit uzunluktadır. Örnek olarak Bitcoin'de işlemler 32 bayt olarak özetlenmektedir.

Elde edilen merkle kökü özet değeri, tüm düğümlerin bir fonksiyonu olduğundan iki veri kümesinin eşit olup olmadığını belirlemede de kullanılmaktadır. Tüm yaprak düğümleri birleştirip özet değerini elde etmek yerine ağaç yapısının kullanılmasının nedeni ise, ağaç yapısının her hangi bir yaprak düğümünün ağacın bir parçası olup olmadığını belirleme konusunda etkin bir yol sağlamasıdır. Örnek olarak N tane işlemin merkle ağacında özetlendiği varsayıldığında, belirli bir alım satım işleminin bloğa dahil olduğunu ispatlamak için log2(N) işlem gereklidir. Her bir alım satım işleminin özet değerinin de 32 bayt olduğu göz önüne alındığında log2(N)*32 bayt özet değeri üretilmesi neticesinde kontrol edilen belirli alım satım işlemini merkle köküne bağlayan doğrulama yolu oluşur. Bu işlem sayısının normal özet değeri listelerinde N olduğu düşünüldüğünde merkle ağacının verimli bir veri yapısı olduğu iddia edilebilir. Blokta saklanan işlemlerin sayısı artıkça bu verimlilik önemli hale gelmektedir. Çünkü kontrol için gereken işlem sayısı taban-2 logaritmasında olduğundan çok yavaş artmaktadır. Tablo 3'te merkle ağacının bahsedilen verimliliği gösterilmektedir. Tablo 3'ten de görülebileceği gibi, blok büyüklüğü hızla artarken bir işlemin bloğa dâhil olduğunu kanıtlamak için gereken doğrulama yolu (merkle yolu) çok daha yavaş artmaktadır.

İşlem Sayısı	**Yaklaşık blok büyüklüğü**	**Doğrulama yolu boyutu (özet değeri)**	**Doğrulama yolu boyutu (bayt)**
16 işlem	4 kilobayt	4 özet değeri	128 bayt
512 işlem	128 kilobayt	9 özet değeri	288 bayt
2048 işlem	512 kilobayt	11 özet değeri	352 bayt
65,535 işlem	16 megabayt	16 özet değeri	512 bayt

Tablo 3: Merkle Ağacı Verimliliği

Şekil 8'de ise bir düğümün, K işleminin bloğa dâhil olduğunu 32 baytlık özet değerlerinden oluşan 128 bayt boyutundaki doğrulama yolu ile kanıtlayabileceği gösterilmektedir. Doğrulama yolu şekilde mavi olarak gösterilen HL, HIJ, HMNOP ve HABCDEFGH olmak üzere dört özet değerinden oluşur. Doğrulama yolu olarak sağlanan bu dört özet değeri ile her hangi bir düğüm, şekilde yeşil olarak renklendirilen HK' nin merkle kökünde içerildiğini şekilde noktalı olarak gösterilen HKL, HIJKL,HIJKLMNOP ve merkle kökü olmak üzere dört ilave ikili özet değeri hesaplayarak ispatlayabilir.



Şekil 8: Doğrulama Yolu (Kaynak: O'REILLY Bitcoin & the Blockchain)

Merkle ağacının sağladığı yapı sayesinde bir düğüm, blok zincirinin tamamına ilişkin veri yerine blok başına 80 bayt gibi küçük boyuttaki blok başlıklarını indirerek her hangi bir işlemin bloğa dahil olup olmadığı kontrolünü tam bir düğümden sadece doğrulama yolunu elde ederek gerçekleştirebilir. Bitcoin'de basitleştirilmiş ödeme düğümleri (SPV), tam blokları indirmek yerine sadece blok üst verilerini indirirler ve dolayısıyla tüm işlemlere sahip değillerdir. Bir işlemin bloğa dahil olduğunu ispatlamak içinse doğrulama yolunu kullanırlar. Örneğin, cüzdanında bulunan bir adrese gelen ödemelerle ilgilenen bir SPV düğümü düşünüldüğünde, SPV düğümü, sadece ilgilenilen adresi içeren işlemleri almak için ağdaki diğer üyelerle olan bağlantılarına filtre oluşturacaktır. Bir üye filtre ile eşleşen işlem gördüğünde, SPV düğümüne "merkleblock" mesajı gönderecektir. "Merkleblock" mesajı, blok başlığını ve ilgili işlemi merkle köküne bağlayan doğrulama yolunu içerir. SPV düğümü işlemin bloğa bağlanması ve bloğa dahil edildiğinin doğrulanması için bu doğrulama yolunu kullanır. SPV düğümü, bloğu, blok zincirin geri kalanına bağlamak için de blok başlığını kullanır. İşlem ile blok arasındaki ve blok ile blok zinciri arasındaki bu iki bağın kombinasyonu işlemin blok zincirine kaydedildiğini kanıtlar. Sonuç olarak, SPV düğümü blok başlığı ve doğrulama yolu için, tam bir bloktan bin kat daha az olan bir kilobayt veri alarak ilgili doğrulama işlemlerini gerçekleştirmiş olur.

4.5 Sınırlamasız Blok Zinciri

Kullanıcıların katılımı açısından blok zinciri uygulamaları sınırlamalı ve sınırlamasız olarak ayrılabilir. Bu bölümde sınırlamasız blok zinciri incelenecek olup sınırlamalı blok zincirine ilişkin detay ise çalışmanın 4.6'ncı bölümünde yer almaktadır.

Sınırlamasız blok zinciri uygulamalarında herhangi bir yetkilendirme süreci yoktur. Yani düğümlerin blok zincirindeki verilere erişebilme veya blok zincirine veri kaydedebilme işlemleri kısıtlanmaz. Ayrıca her düğüm, blok zincirinin sonuna eklenecek bir sonraki bloğun nasıl yapılandırılacağına karar verilmesi konusunda fikir birliğine sürecine katılma hakkına sahiptir. Sınırlamasız blok zinciri uygulamalarının merkezi bir karşı tarafa veya güvenilir katılımcılara ihtiyacı yoktur. Çünkü bunun yerine güven matematiksel fikir birliği algoritmaları ile sağlanır. Sınırlamasız blok zinciri uygulamalarındaki fikir birliği protokollerinde düğümler arasında güven açısından herhangi bir fark gözetilmediğinden bu tip uygulamalarda kullanılan fikir birliği protokolleri genellikle iş ispatı gibi kripto-ekonomik süreçlere dayanır. Bu tür blok zinciri uygulamaları Bitcoin ve Ethereum gibi katılım kısıtlaması bulunmayan ve tamamen dağıtık mimarideki açık sistemlerdir.

Sınırlamasız blok zinciri uygulamalarının, genellikle Bitcoin gibi zincir üzerinde yaratılmış varlıklar için pratik olduğu söylenebilir. Çünkü zincir dışı varlıkların doğrulayıcılar tarafından zincirde yaratılan varlıklarla aynı şekilde kontrol edilmesi mümkün değildir ve zincir dışı varlıkların işlemlerinde ortaya çıkan anlaşmazlıkların dış bir tüzel varlık tarafından çözülmesi gerekebilir. Bu argümanlar finansal kurumları sınırlı blok zinciri uygulamalarına yöneltmek için güçlü olsa da finansal kurumlar sınırsız zincirler tarafından benimsenen fikir ve kavramları görmezden gelmekten kaçınmalıdır. Örneğin bu tarz uygulamaların tüm insanlar tarafından kullanılabilir olması öngörülemeyen ağ etkisi kazanmalarına neden olabilir. Ayrıca yıkıcı yeniliklerin, ürünleri henüz kanıtlanmamış olduğundan genellikle ilk müşterilerini piyasa tabanından bulduğu ve iyileştirmelerle müşteri tabanını genişleterek nihayetinde endüstrileri yeniden şekillendirmeye dahi neden olabildikleri, sınırlamasız blok zinciri uygulamalarını değerlendirirken finansal kurumlar tarafından göz önüne alınmalıdır.

4.6 Sınırlamalı Blok Zinciri

Finansal piyasalar, menkul kıymet ihraççısının işi ile doğrudan ilgili olmayan operasyonel ve karşı taraf riski gibi riskleri önlemek için yasal anlaşmalar ve düzenlenmiş usuller aracılığı ile karşılıklı güven veren kurumların bir ağı olarak zaman içinde gelişmiştir ve bu piyasada hemen hemen her kurum, düzenleyici kurumların denetimi ve gözetimi altındaki hesap verme yükümlülüğü bulunan yetkilendirilmiş karşı taraflarla işlem gerçekleştirmektedir. Ayrıca Bitcoin ağının amaçları için çok önemli olan, piyasa katılımcıları için takma ad kullanılması, sistemin denetlenemez olması, zincirin dünyanın her yerinden herkes tarafından erişilebilir olması ve gerçekleşen yasadışı işlemlerin iptal edilememesi gibi özellikler finansal piyasalar için

geçerli değildir. Bunun yerine, piyasa katılımcılarının karşılaması gereken standartlara uyumlu bir sisteme ihtiyaç vardır. Bütün bu şartlar da ilk olarak Bitcoin'in güçlü tarafını oluşturan teknoloji olarak adını duyuran blok zincirinin, daha sonra dallanarak birçok farklı deneysel forma geçmesi sonucu oluşan piyasa oyuncuları arasında sınırlamalı blok zinciri teknolojisinin uygulanması için alan oluşturmuştur.

Buterin[20] tarafından sınırlamalı blok zinciri uygulamalarının tamamen sınırlı zincirler ve konsorsiyum zincirleri olarak ikiye ayrılabileceği ifade edilmektedir. Her iki durumda da, blok zincirindeki yönetim birimleri (paylaşılan defterler dahil) önceden tanımlanmış belirli ölçütlere göre yeni katılımcıların kabulünü onaylar ve doğrulama işleminden sorumlu düğümleri belirtir. Konsorsiyum zincirlerinde fikir birliği sürecini tek başına kontrol edebilen tek bir düğüm yerine blok zincirine eklenecek bir sonraki bloğu doğrulayan bir dizi belirlenmiş düğüm olduğundan sistemin kısmen merkezi olduğu söylenebilir. Bu sistemde, okuma ve yazma izinleri tamamen herkesi açık olacak şekilde veya herkes okuma iznine sahipken sadece belirli düğümlerin yazma izni olacak şekilde ayarlanabilir. Tamamen sınırlı blok zincirlerinde ise blok oluşturma ve yazma izinleri tek bir düğümle ile sınırlı iken okuma izinleri herkese açık veya sınırlı olacak şekilde ayarlanabilir.

4.7 Sınırlamalı-Sınırlaması Blok Zinciri Genel Değerlendirme

Şartlara bağlı olarak sınırlamasız ve sınırlı blok zinciri uygulamalarının kendi avantajları ve dezavantajları vardır. Sınırlamasız blok zinciri uygulamalarının tek bir varlık tarafından kontrol edilmemesi ve kullanıcıları arasında herhangi bir güven gerektirmemesi suiistimal riskini azaltır. Ayrıca bu sistemde yeni yazılımların kabul edilmeye ve kullanılmaya başlanması tamamen sisteme bağlı olduğundan kullanıcılar bir şekilde yazılım geliştiricilerden de korunur. Sınırlamasız blok zincirlerinin herkese açık olması, veri kaybı ve kötü niyetli kullanıcıların sistemi ele geçirme riskinin kullanıcı sayısı artıkça azalmasına yol açmaktadır. Yine bu sistemde hiç kimse zinciri tek başına kontrol etmediğinden işlemleri geri almak ve sistemin kurallarını hızlı bir şekilde değiştirmek mümkün değildir. Bu özellik kripto-para örneğinde bir avantaj olarak görülebilir ancak örneğin birbirleri ile veri paylaşmak isteyen bankalar arasında oluşturulan bir blok zinciri uygulamasında zincirin kontrolünün katılımcıların hepsine bırakılması genellikle pek uygun değildir. Bu gibi durumlarda, sınırlı blok zinciri çözümünün tartışılabilir bir biçimde daha uygun olduğu söylenebilir.

Sınırlamalı blok zincirinde, katılımcıların kimliğinin en azından yönetim organı tarafından bilinmesi, haksızlığa yol açabilecek herhangi bir yanlış davranışın tanımlanabileceğini ve bu yanlış davranışın cezalandırılabileceğini ifade etmektedir. Ayrıca sınırlamalı blok zinciri katılımcıların zincirde gerçekleştirdikleri işlemlerin yanı sıra uygulama dışında da gerçekleştirdikleri işlemler açısından da uymaları gereken kurallar bulunmaktadır. Yani sınırlamalı blok zincirleri, geleneksel finans sisteminde yüksek düzeyde olan şeffaflık ve hesap verilebilirliğin bir örneğini oluşturmaktadır. Diğer taraftan sınırlamasız blok zinciri kullanıcılarının ise tanım

[20] Vitalik Buterin. On Public and Private Blockchains.

gereği, sistemdeki faaliyetleri nedeniyle zincir dışında sorumluğu bulunmamaktadır. Para cezası ve itibar kaybı gibi tedbirler ise katılımcıların kimliği bilinmediğinden dolayı yine sınırlamasız blok zincirinde uygulanabilir değildir.

4.8 Genel Olarak Fikir Birliği Algoritmaları

Blok zinciri kullanıcıları tarafından gönderilen yeni işlemler, ağda bulunan belirli sayıdaki doğrulayıcı düğüm tarafından doğrulandıktan sonra diğer kullanıcılar güncellemeyi alır ve buna göre zincirin lokal kopyasını değiştirirler. Doğrulayıcılar, bir işlemle gönderilecek varlıkların işlemi başlatan tarafta mevcut olup olmadığını en son bilgilere göre kontrol etmelidir. Bu nedenle, işlemi başlatan taraf doğrulayıcılara, ne kadar varlığın kime gönderileceği gibi standart bilgilere ek olarak blok zincirinin son versiyonuna ilişkin özet değeri ile doğrulama yolu gibi bilgileri de sağlamalıdır.

Doğrulama kuralları genel olarak, siber esneklik ve verimlilik arasındaki dengede tatminkâr bir uzlaşma bulmaya çalışmaktadır. Bu nedenle sistemde hem ekonomik teşviklerden hem de kriptografik güvenlik özelliklerinden yararlanılmaktadır.

Sınırlamasız bir ağda, doğrulama hakkını kişi başı bir oy temelinde paylaşmak teorik olarak imkânsızdır. Çünkü her hangi bir kullanıcı işlemlerin tek taraflı olarak onaylanmasına imkân sağlamak veya ağa hizmet engelleme saldırısı yaparak yasal işlemlere hizmet reddi uygulanmasına neden olmak amacıyla birden fazla ağ adresi oluşturabilir.[21] Blok zinciri uygulamaları, bu problemleri çözmek için bir dizi fikir birliği algoritmaları kullanmaktadır. Bu algoritmalardan blok zinciri uygulamalarında yaygın olarak kullanılan işin kanıtı (proof of work) algoritması çalışmanın 4.9'uncu bölümünde, hissenin kanıtı (proof of stake) algoritması ise çalışmanın 4.10'uncu bölümünde incelenmektedir.

Genel olarak fikir birliği algoritmaları, blok zinciri ağındaki katılımcılar arasında güven ihtiyacını ortadan kaldıran tekniklerdir. Bu algoritmalar, blok zinciri ağındaki tüm düğümlerin her bir güncellemede aynı işlem kümesinin blok zincirine eklenmesini sağlamak amacıyla kullanılır. Fikir birliği algoritmaları, uygulamanın özelliklerine bağlı olarak farklı şekillerde tasarlanabilir. Ancak kullanılan fikir birliği algoritması, uygulamanın ölçeklenebilirliğini ve verimliliğini büyük ölçüde etkilemektedir.

Algoritmalar arasındaki temel ayırt edici faktör algoritmanın olasılıksal veya deterministtik olmasıdır. Olasılıksal algoritmada, blok zinciri ağındaki tüm düğümler bir sonraki bloğu üretmeye çalışırlar[22]. Her bir düğümün, bir sonraki bloğu üretebilmesine ilişkin münferit olasılığı ve dolayısıyla blok zinciri üzerindeki etkisi kullanılan olasılıksal algoritmaya göre farklılaşmaktadır. Olasılıksal olmayan algoritmalarda ise hangi işlemlerin bir sonraki blokta yer alacağını belirlemek için

[21] Sybil saldırısı olarak bilinen bir strateji.
[22] Yaygın olarak madencilik olarak atfedilir.

deterministtik bir süreç kullanılır. Yani bir sonraki bloğun hangi düğümde üretileceğini tahmin etmek mümkündür.

Olasılıksal bir algoritma kullanıldığında, iki farklı düğümün hemen hemen aynı anda bir blok oluşturma ihtimali vardır. Bu da blok zincirinde, ağın farklı bölümlerinde farklı blokların kabul edildiği çatal olarak adlandırılan durumun oluşmasına yol açar. Olasılıksal fikir birliği algoritmalarında çatallanma problemi genellikle, bir düğümün daima ve yalnızca üzerinde en fazla bloğa sahip olan çatalda çalışması gerektiğini söyleyen bir kurala sahip olmakla çözülür. Yani bir çatal yeni bir blok üretir üretmez ağdaki bütün düğümler bu çatala geçecek ve blok zinciri yeniden birleştirilecektir. Terk edilmiş çataldaki bloklar atılacak ve yalnızca atılan bloklarda bulunan işlemler tersine çevrilecektir.

Olasılık protokolünde kullanıcı, bir işlemin çatallanma nedeniyle atılmayacağından tamamen emin olamaz. Ancak bunun gerçekleşme riski, daha fazla blok oluşturulduğunda ve işlem blok zincirinde daha derinlere yerleştiğinde azalmaktadır. Bu nedenle, örneğin Bitcoin ağında bir işlemin nihai olduğundan emin olmak için en az altı blok beklenilmesi önerilir. Bu özellik genellikle blok kesinleştirme olarak adlandırılır. Olasılıksal protokollerde sadece olasılık bakımından blok kesinleştirme hakkında konuşabilirken deterministtik protokollerde anlık blok kesinleştirmesi vardır.

4.9 İşin Kanıtı (Proof Of Work)

Belki de en olasılıksal fikir birliği süreci, her kullanıcıya bir oy hakkının verildiği ve tüm kullanıcıların bir sonraki bloğa hangi işlemlerin dâhil edileceğine yönelik olarak bu oy hakkını kullandığı yöntemdir. Bu yöntemde en fazla oyu alan işlemler seti bloğa dâhil edilir. Ancak bu sistem Sybil saldırısı[23] denilen duruma karşı savunmasızdır. Çünkü bir kullanıcı birden fazla hesap oluşturarak sistemde orantısız miktarda etkiye sahip olabilir. Bitcoin'in yaratıcısı Nakamoto bu sorunu, kullanıcının etkisini fiziki miktar yerine kullanıcının erişebildiği CPU gücü cinsinden enerji miktarına dayandırarak çözdü. Bu tür bir fikir birliği süreci ise genellikle "işin kanıtı" olarak adlandırılmaktadır.

PoW'un genel fikri Bitcoin ile birlikte değil, daha önce Dwork ve Naor tarafından önemsiz e-posta ile mücadele etmek için bir ağ üzerinden mesaj gönderme işlemine CPU gücü şeklinde bir maliyet ekleyerek önerildi (Dwork 1993). Bu yöntemle tek bir mesaj göndermek, normal kullanıcıyı etkilemezken büyük miktarda mesaj göndermek maliyetli olacaktır.

PoW sistemi, tersine çevrilemeyen özetleme fonksiyonlarını içeren çözülmesi zor ancak çözümü kolayca kontrol edilebilen matematiksel problemlere dayanmaktadır. Bu tarz problemlerin çözümünün bulunması, problemler sadece yinelemeyle çözülebildiğinden matematiksel yetenekten ziyade şans ve hesaplama

[23] Sybil saldırısı, ağdaki bir düğümün birden fazla kimliği talep ettiği bir güvenlik tehdidi türüdür.

çabası meselesidir. Yani PoW sistemi yoğun hesaplama gücü ve enerji gerektirmektedir.

PoW sistemi büyük ölçüde Back'in "hashcah" fikrine dayanmaktadır. Verileri paylaşmak için blok zincirini kullanan eşler arası ağda, iş ağda yeni bir blok yayınlama eylemine eklenir. İş genellikle nesne olarak anılan maliyet fonksiyonunun hesaplanması suretiyle yapılır. "Hashcash" fikrinde bu maliyet fonksiyonunun özellikleri şu şekildedir:

- Etkileşimsiz, yani her düğüm nesne hesaplamaya diğer düğümlerden her hangi bir bilgi almadan başlayabilir.
- Gizli kapısız, yani nesneyi hesaplama açısından hiçbir düğümün diğer düğümlere karşı bir avantajı yoktur.
- Genel olarak denetlenebilir, yani herhangi bir gizli kapı veya bilgi kullanmaksızın, işin yapıldığı üçüncü taraflarca verimli bir şekilde doğrulanabilir.
- Nesne hesaplamanın olasılık maliyetine bağlı değildir, yani teorik olarak, nesneyi bulmama ihtimali, ortalama süre geçtikçe sıfıra doğru gitse de nesneyi hesaplamanın ne kadar süreceği konusunda herhangi bir üst sınır yoktur.

PoW sisteminde her bir doğrulayıcı, standart kayıt /muhasebe sistemi kurallarına uyduğu için yasal olarak görülebilecek bekleyen işlemler oluşan bir grup seçer ve bu işlemleri blok zincirinin mevcut güvenilir versiyonuna ekler. Bu şekilde elde edilen yeni versiyonu maliyet fonksiyonun girdisi olarak kullanır. Maliyet fonksiyonunu oluşturan matematiksel probleme çözüm bulununca blok zincirinin yeni versiyonu ile birlikte bulunan çözüm ağın geri kalan düğümlerine gönderilir. Diğer ağ katılımcıları ise;

- Güncelleştirmenin yalnızca yasal işlemleri içerip içermediğini,
- Doğrulayıcın matematik problemine ilişkin çözümü çalışarak bulup bulmadığını

kontrol eder. Eğer her iki koşulda sağlanırsa, doğrulayıcılar blok zincirinin yeni versiyonu hakkında mutabakata varırlar ve bu versiyon sistemde bekleyen diğer işlemleri doğrulamak için başlangıç noktası olarak kullanılır.

Doğrulayıcılar, matematiksel maliyet fonksiyonunu çözmek için gerekli donanım ve elektrik maliyetine katlanırlar. Sistemde çözümü ilk bulana ödül verildiğinden işlemleri doğrulama görevi doğrulayıcılar tarafından rekabetçi bir temelde ele alınır. Örneğin, Bitcoin uygulamasında bu ödül Bitcoin olarak verilmektedir.

PoW sistemlerinde belirlenen matematiksel problemin tek amacı doğrulama işlemini pahalı hale getirerek hesaplama gücü temelinde oylama yapısı oluşturmaktır. Yetkili/kabuledilen blok zinciri, ağda yer alan kullanıcılar tarafından yayınlananlar arasından doğrulanmış güncelleştirmeler geçmişi en uzun olan dolayısıyla matematiksel fonksiyonunun çözümü için en fazla hesaplama kapasitesini gerektiren

versiyondur. Doğrulama maliyeti her hangi bir katılımcının işlemleri hızlı bir şekilde doğrulamasını engellemek için düzenli olarak ayarlanır. Böylelikle beklenen şartlar altında, kötü niyetli bir kullanıcının yalnızca yeni işlemleri ağın geri kalanından daha hızlı doğrulayabildiği durumda blok zincirini bozabilir. Yani sadece sistemdeki tüm doğrulayıcıların sahip olduğu toplam hesaplama gücünün yarısından fazlasına sahip olarak sistemin bozulması mümkündür.[24]

PoW aracılığı ile doğrulanan işlemler, blok zincirine yapılan saldırıların yalnızca ekonomik nedenlerden kaynaklandığı konusundaki göz ardı edilemez varsayım altında görece güvenlidir. Ancak sistemdeki varlığın[25] değeri artıkça kötü niyetli kullanımdan beklenen gelirde artar. Böylece ağdaki toplam hesaplama gücünün herhangi bir yüzdesine ulaşma maliyeti de aynı faktöre bağlı olarak artar. Bu durumda, potansiyel saldırganların, elde edebilecekleri gelir büyüdüğünden ağdaki hesaplama kapasitesinin çoğunluğunu kontrol etmek için daha fazla kaynak yatırmaya teşvik edildiği doğrudur. Fakat ayrıca, doğrulayıcılar tarafından elde edilecek gelirle orantılı olarak ödülü alabilmek için hesaplama kapasitelerini artırmaya yönelik uygun yatırımlar yapılır. Yani ağdaki varlığın değeri artığında blok zincirinin tahrif edilmesinden beklenen gelirde artacak ancak doğrulayıcıların değer artışına bağlı olarak doğrulama kapasitelerine yapacakları yatırımların da artacağı göz önüne alındığında ağın sahip olduğu hesaplama kapasitesinin %50'sini elde etme maliyeti de artacaktır[26]. Dolayısıyla blok zincirini tahrif etmek için yapılan girişim ekonomik açıdan karlı değildir.

Bazı doğrulayıcılar tarafından blok zincirine eklenilmek istenilen işlem kümesinin PoW'u, diğer bir doğrulayıcının ayrı bir işlem setine yönelik PoW'u çözerek blok zincirini güncellemesinden sonra çözülebilir. Bu durumda blok zinciri değiştiğinden doğrulayıcılar ödülü kaybeder ve bu doğrulayıcıların işlemleri blok zincirine eklenemez. Bu nedenle bu işlemler, bekleyen işlemler kümesine geri döndürülürler ve bu işlemler için güncellenen blok zincirine dayanan yeni bir matematiksel problem tanımlanır.[27]

Özet olarak, PoW Bitcoin de dahil olmak üzere genellikle sınırlamasız blok zinciri uygulamalarında kullanılan bir algoritmadır. Bu algoritmada, blok zinciri ağında verileri gönüllü olarak doğrulayan "tam düğümler" bulunmaktadır. Maliyet fonksiyonunu en hızlı çözerek işlem kümesini doğrulayan gönüllü düğümlere dijital varlık türünden teşvik verilmektedir. Bu algoritmanın kötü niyetli kullanıma karşı

24 Kötü niyetli bir kullanıcının, diğer doğrulayıcıların teşviklerinde değişiklik yaptığı durumda ağa saldırabilmek için bilgisayarın% 25'ini elinde bulundurması yeterlidir. Bkz. Eyal ve Sirer (2014).

25 Kriptopara vb.

26 Bitcoinwiki. Proof-of-Stake. https://en.bitcoin.it/wiki/Proof_of_Stake.

27 Başarısız doğrulamada kullanılan hesaplama gücünün boşa harcanmasından ziyade saldırı için gerekli olan hesaplama gücünü artırmak için kullanılmasına izin vermek amacıyla standart PoW'da değişiklikler geliştirilmektedir. Bkz. Sompolinsky and Zohar (2013). Zamfir, Ethereum blogunda basitleştirilmiş uygulamaları anlatıyor.

dayanıklı olması güçlü yönü olarak ortaya çıkarken çok yüksek miktarda hesaplama gücü ve enerji kullanımı gerektirmesi algoritmanın zayıf yönünü oluşturmaktadır.

4.10 Hissenin Kanıtı (Proof of Stake)

Saldırılara karşı korumayı daha da artırmak ve PoW tabanlı uzlaşım sistemi tarafından gerekli olan yüksek miktardaki enerji tüketimini azaltmak için Bitcoin geliştirici topluluğu tarafından "hissenin kanıtı" (PoS) fikri geliştirildi. Bu sistemde bir düğümün blok zinciri üzerindeki etkisi, PoW sisteminde olduğu gibi hesaplama gücü ile değil de düğümün blok zincirindeki kayıtlı varlıkları ile orantılıdır. PoS fikri, blok zincirindeki pay sahipliği büyük olan düğümlerin blok zincirine olan güveni koruma ve dostça bir düğüm olarak çalışma konularında daha istekli olacakları varsayımı üzerine kurulmuştur.

PoS sisteminde doğrulayıcıların hisselerinin nasıl ölçüleceği ise sistemin kritik yönünü oluşturmaktadır ve bu ölçüm için farklı yaklaşımlar kullanılmaktadır. Doğrulayıcıların hissesini ölçmek için kullanılan bazı olası ölçütler şunlardır:

- Sahip olunan blok zincirine özgü varlık miktarı.
- Sahip olunan blok zincirindeki belirli varlık miktarı ya da blok zinciri dışındaki varlıkların teminat olarak miktarı.
- Veya sınırlı blok zinciri uygulamalarında doğrulayıcının itibarı.

Blok zinciri uygulamalarının ağa katılım açısından sahip oldukları çeşitli özellikler, ağın verimliliğini dolaylı olarak etkiler. Her katılımcının blok zincirinin korunması için fazla kaynak ayırması yerine blok zincirini koruma yükümlülüğü, yasalara karşı davranışının cezalandırılacağını bildiğinden iyi niyet kuralları çerçevesinde hareket edecek katılımcılara bırakılabilir. Böylece sınırlı blok zinciri uygulamalarının geliştiricileri, sınırsız blok zinciri uygulamalarında gerekli olanlardan daha az maliyetli fikir birliği algoritmalarını kullanmayı tercih edebilir. Bu şekilde, sınırlı blok zinciri uygulamalarında doğrulama işlemi tüm katılımcılar için maliyetli hale getirilmez ancak saldırganlar için sistemi ele geçirmek hala maliyetli kalmış olur.

Teminatlı PoS sisteminde, doğrulayıcıların teminatları blok zinciri dışındaki güvenilir üçüncü taraflarca saklanır. Her hangi bir doğrulayıcının uygun olmayan bir işlemi onaylamaya teşebbüs ettiği ispatlandığında ise, teşebbüsün başarılı olup olmamasına bakılmadan teminatlarından ceza tahsis edilir. Ayrıca bu doğrulayıcıların dijital imzaları kara listeye alınır ve teminatlardan tahsis edilen ceza sistemin mülkiyetine geçer.

Finansal piyasa altyapıları ve aracılar tarafından oluşturulan kapalı bir ağda, yeni işlemlerin doğrulanması için iyi niyetli doğrulayıcıların üçte ikisinin onayının aranması görece güvenli olarak kabul edilebilir. Çünkü bu sistemde, ağa saldırmayı planlayan bir tarafın, yeni işlemlerin blok zincirine doğru şekilde kaydedilmesine müdahale edebilmesi için doğrulayıcı olarak davranan finansal kuruluşların üçte birinden fazlasının kontrolünü ele geçirmesi gerekecektir. Ancak yine de siber esneklik açısından, bu tarz güvenliklerin merkezi veritabanlarında sağlananlardan

daha güçlü veya zayıf olup olmadığı açık değildir. Bu durum siber saldırının, merkezi bir sistemi ele geçirme veya farklı güvenlik standartlarına sahip olabilen blok zinciri doğrulayıcılarının üçte birinden fazlasını ele geçirebilme olasılığına bağlıdır. Bazı fikir birliği protokollerinde ise, düğümlerin sistemi kontrol altına almayı amaçlayan saldırgan tarafından aşamalı olarak ele geçirilmesi riskini azaltmak için ağın çoğunluğuyla hemfikir olmayan düğümlerin derecesini otomatik olarak düşürülür.

Yeni işlemler doğrulandıktan ve blok zincirinin son versiyonuna eklendikten sonra blok zinciri uygulamasının özelliğine bağlı olarak kararlaştırılmış[28] veya beklemede olarak sayılabilir. Yani işlemler doğrulandıktan sonra belirli bir süre boyunca, bekleyen blok zinciri güncelleştirmeleri iptal edilebilir. Bu durum genellikle sınırlamalı blok zinciri uygulamalarında uygulanmaktadır. Bu nedenle sınırlamasız blok zinciri uygulamalarının bazı geliştiricileri tarafından, bilinmeyen taraflara açıklıktan ziyade takasın nihai olması ve blok zincirinin bakım maliyetiyle ilgilenen finansal kurumların ihtiyaçlarını karşılamak için kısıtlanmış teknolojilere geçileceği açıklanmıştır.

PoS sistemlerinde ele alınması gereken diğer bir husus ise blok zincirinin çatallanmasının düşük maliyetli olmasıdır. Blok oluşturma işlemine neredeyse hiç hesaplama işi eklenmediğinden kolayca oluşabilen çatallanma, kötü niyetli düğümlerin çifte harcama yapabilmelerini, açgözlü düğümlerin tüm çatallarda çalışarak daha fazla ödül alabilmelerini mümkün hale getirmektedir. Bu da sistemin çatallanması konusunda doğal bir teşvik oluşturmaktadır. Bu problemle mücadele etmek içinse birçok PoS uygulaması "kontrol noktası" kavramını getirmiştir Bir kontrol noktası bloğundan önce oluşturulmuş bloklar artık revize edilemez ve bu nedenle bu bloklardaki tüm işlemler çift harcama saldırılarına karşı güvenli hale gelir[29].

28 Tüm katılımcılar tarafından nihayet ve geri alınamaz bir şekilde üzerinde anlaşmaya varılmış.
[29] Nxt. Nxt Whitepaper. http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt.
Scott Nadal Sunny King. Peercoin Whitepaper. https://www.peercoin.net/whitepaper.

5. MENKUL KIYMET PİYASALARINA UYGULANAN DLT'NİN OLASI FAYDALARI

Bu bölümde menkul kıymet[30] piyasalarında DLT kullanımının muhtemel faydaları analiz edilmektedir. Ancak hemen belirtmek gerekir ki, teknoloji hızla geliştiği için gelecek yıllarda yeni faydalar ile karşılaşılabilir. DLT uygulamalarının olası zorlukları ve sınırlamaları ise çalışmanın 6'ncı bölümünde tartışılmaktadır.

5.1 Takas ve Takas Öncesi İşlemler

DLT kullanımı ile aracıların sayılarının azaltılması ve mutabakat sürecinin daha verimli hale getirilmesi suretiyle bazı finansal işlemlerin takas ve takas öncesi işlemler sürecinin hızlandırılması sağlanabilir. Özellikle de DLT, fazla aracıya olan ihtiyacı azaltarak tarafların ülkeler arasında birbirleri ile daha kolay işlem yapmasını sağlayabilir. DLT ağının tüm katılımcılarının ağın kalanı ile tutarlı olacak şekilde kayıtların lokal kopyasını elinde tutması ve işlemlerin onaylanması için fikir birliği algoritmalarını kullanılması anlamına gelen blok zincirinin dağıtılmış mimarisi sayesinde, mutabakat süreci daha hızlı ve verimli şekilde yapılabilir. Ayrıca DLT kullanımı sayesinde, işlemlerin takas öncesi işlemleri ile takas işlemlerinin tek bir adımda neredeyse anlık olarak birleştirilebilir ki bu da karşı taraf riskinin azalması ve teminat gönderme gereksinimin azalması gibi bir takım ek avantajlar yaratılabilmesi anlamına gelmektedir

5.2 Varlıkların Saklanması ve Sahiplik Kayıtları

DLT sistemi, menkul kıymetlerin sahipliğinin kayıt altına alınması ve saklanmasını, benzersiz referans veri tabanı sistemi kullanarak, sözleşme koşullarının olası belirsizliklerini azaltarak, işlemlerin otomatikleştirilmesini sağlayarak ve mutabakat sürecini verimli hale getirerek kolaylaştırabilir.

DLT menkul kıymet piyasalarında, sisteme gömülü olacak şekilde benzersiz güvenlik tanımlayıcısı kullanmak gibi eşsiz bir referans sisteminin uygulanmasını kolaylaştırabilir. Bu tanımlayıcı daha sonra ağdaki tüm katılımcılar tarafından paylaşılabilir ve kullanılabilir. Bununla birlikte, ISIN gibi çeşitli standart tanımlayıcıların farklı varlık sınıfları için hâlihazırda kullanıldıklarını dolayısıyla bu özelliğin yeni olmayacağını belirtmek gerekir. Ancak DLT tarafından, bu benzersiz referans sistemlerinin işlemlerin yaşam döngüsünün entegre bir parçası yapılabilmesi mümkündür.

Kısa vadede kullanımları belirli araçlar veya sözleşmelerle sınırlı olsa da blok zinciri sisteminin üzerine oturacak "akıllı sözleşmeler", en azından normal sözleşmeye bağlı belirsizliklerin azaltılmasına ve kurumsal işlemlerin otomasyonunun artırılmasına katkı sağlayabilir. Akıllı sözleşme kavramı DLT'nin gelişmesinden önce ortaya çıkmıştır ancak bu teknoloji kavramın gelişimini hızlandırabilir. Akıllı sözleşmeler, belirli bir sözleşmenin koşullarını yerine getirmek amacıyla kendi

[30] Bu çalışmada "menkul kıymetler" terimi finansal araçlar olarak kullanılmıştır.

kendine çalışan kodları ifade etmektedir ve ödeme esasları ile gizlilik anlaşmaları gibi sözleşme şartlarını etkili bir şekilde hesaplama materyaline çevirirler

Daha öncede belirtildiği gibi, paylaşılan yapısı ve fikir birliği algoritmalarının kullanılması nedeniyle DLT, mutabakatları da daha verimli hale getirebilir.

DLT ayrıca dijital menkul kıymetleri ihraç etmek, sahipliklerini izlemek ve ihraç ile ilgili hizmetleri desteklemeye yardımcı olmak için kullanılabilir.

Sonuç olarak blok zincirinin menkul kıymetlerin saklanması ve sahiplik kayıtlarının izlenmesi için güvenilir bir kaynak haline gelme potansiyeli bulunmaktadır. Bunun ise mevcut durumda piyasa katılımcıları/ altyapıları tarafından kullanılan mutabakat sistemleri ve menkul kıymet sahipliğinin izlendiği bazı merkezi sistemlerin gereksiz hale gelmesi ve saklamacıların rollerinin değişmesi gibi etkileri olabilir.

5.3 Raporlama ve Gözetim

DLT sayesinde, tek bir kaynaktan edinilen bilgiyle kıyaslandığında mevcut bilgi içeriğinin kapsamının genişletilmesi ve bu bilgiye daha hızlı erişim imkânı sağlanması suretiyle; raporlama, risk yönetimi ve denetim amaçlı verilerin toplanması süreci verimli hale getirilebilir. DLT kullanımı ile teoride her kayıt geçmiş versiyonları ile görülebilmektedir. DLT'nin bu özelliği gerekli önlemlerin alınması koşuluyla, raporlama görevlilerine, risk yöneticilerine ve düzenleyicilere birçok kolaylık sağlayabilir. Ayrıca, DLT'nin bu bilgilere erişim hızını artırabilmesi de mümkündür. Örnek olarak, denetleyici makamların DLT sisteminde bir düğüm olması ve DLT'de tutulan bilgilere doğrudan erişim sağlayabilmesi söz konusudur.

5.4 Karşı Taraf Riski

DLT kullanımı ile bazı menkul kıymet işlemleri ile ilgili karşı taraf riski azaltılabilir. Daha öncede açıklandığı gibi DLT işlemlerin takas döngüsünü kısaltabilir. Bu ise işlem taraflarının, karşı tarafın temerrüde düşme riskine daha kısa süre maruz kalması anlamına gelmektedir. DLT'nin bazı işlemlerin karşı taraf riskini ortadan kaldırabileceği ve takasın anlık olması nedeniyle MKT ihtiyacını da ortadan kaldırabileceği tartışılmaktadır. Bu noktada, spot işlemler ile türev işlemler gibi vadeli işlemler arasındaki ayrımı yapmak önemlidir. Çünkü spot işlemler için tek bir takas işlemi ilgili tarafların yükümlülüklerini bir defada ortadan kaldırırken türev işlemlerde yükümlülükler sözleşmenin süresi boyunca devam eder ve sözleşme süresince karşı taraf riskini azaltmaya ihtiyaç vardır. Bu nedenle, DLT'nin spot işlemlerde karşı taraf riskini ortadan kaldırma potansiyeli olsa da türev işlemlerle ilgili karşı taraf riskini kaldırması olası olmadığından MKT'nin türev araç işlemlerindeki rolünün değişmeyeceği[31] değerlendirilmektedir. Ayrıca, karşı taraf riskini azaltmak için işlemler gerçekleştirilirken teminat alışverişine hala ihtiyaç duyulacaktır.

[31] MKT, Türev ürünler için DLT kullanımı ile kaybolabilecek netleştirme gibi ek faydalar da sağlamaktadır. Bkz. 6.1

5.5 Etkin Teminat Yönetimi

Daha öncede belirtildiği üzere DLT kullanımının spot işlemlerde karşı taraf riskini azaltma hatta ortadan kaldırma potansiyeli bulunmaktadır. Böylece piyasa katılımcıların, belirli işlemler için daha kısa süre daha az teminat göndermesi veya hiç teminat göndermemesi mümkün olabilir. Ancak hâlihazırda spot işlemlerin büyük bir kısmı teminatsız olarak yapılmaktadır ki bu da DLT'nin bu alandaki faydasını sınırlandırmaktadır.

DLT ayrıca, piyasa katılımcıları arasındaki teminat hareketlerinin iyileştirilmesi için de kullanılabilir. Bu iyileştirme ile de teminat ihtiyacının azalması ve teminat hareketlerinin hızlandırılması sağlanacaktır. Bu ise piyasanın teminat kullanılabilirliğini artıracak ve piyasa katılımcıları teminatı daha sık kullanabilecektir.

5.6 Kullanılabilirlik

DLT sisteminin, dağıtılmış mimarisinden dolayı teorik olarak sürekli çalışabilir bir sistem olduğu ifade edilebilir. Sistemde mevcut olan bu yüksek seviyedeki kullanılabilirlik ise, süreçlerin toplu halde organize edildiği finansal hizmetler için potansiyel bir fayda olarak görülebilir.

5.7 Güvenlik ve Esneklik

DLT sistemi potansiyel olarak çok güvenli bir teknoloji olarak sunulmakta, hatta bazıları tarafından DLT'nin mevcut sistemlerden daha güvenli olduğu savunulmaktadır. Esas itibariyle test edilme ihtiyacı olmakla birlikte DLT'nin algılanan yüksek güvenlik seviyesi sistemin dağıtılmış olma niteliğine dayanmaktadır. Yani dağıtılmış yapı nedeniyle tek bir saldırısı noktası bulunmamaktadır ve sisteme yönelik bir saldırının sistemin tamamını çalışamaz hale getirmesi için sistemdeki tüm noktaları hedef alması gerekmektedir. Ayrıca işlemlerin güvenliğinin sağlanması ve doğrulanması için de kriptografi ve fikir birliği algoritmaları kullanılmaktadır. Bu özellikler siber saldırı riskini azaltmaktadır. Ek olarak kayıtların aynı anda farklı lokasyonlarda tutulacak olması kurtarma planlarına olan ihtiyacı da azaltmaktadır.

5.8 Maliyetler

Genel bir maliyet düşüşü, DLT'nin öne çıkan en önemli faydalarından biridir. Örneğin işlem sonrası faaliyetlerde, mevcut durumda manuel olarak yapılan bazı işler DLT kullanımı ile otomatikleştirerek orta ve arka ofis süreçlerini hızlandırabilir ve dolayısıyla maliyetler azaltılabilir. Aynı durum raporlama ve izleme işlevleri için de geçerlidir. Ayrıca DLT kullanımı, şirket düzeyinde tutulan münferit defter yerine, kayıtların sisteme dağıtılmasıyla mutabakatlaşma maliyetini azaltabilir veya hatta ortadan kaldırabilir. Ayrıca sistemin dağıtık mimaride olması sistemin çalışamaz duruma gelmesini oldukça zorlaştırmakta ve bu da DLT kullanımı ile maliyeti oldukça yüksek olan iş sürekliliği planlarına olan ihtiyacın azalabileceğini göstermektedir. Buna ek olarak DLT, birden fazla aracıya duyulan ihtiyacı azaltma potansiyeline sahip olduğundan, genel olarak işlem maliyetlerini de azaltabilir.

5.9 Diğer Olası Faydalar

DLT şeffaf yapısı sayesinde potansiyel alım satım kazançlarını ilan etmek suretiyle işlem öncesi bilgileri geliştirmek ve fikir birliği algoritmaları kullanması sayesinde de karşı tarafların sahiplik doğrulaması yapmasını sağlayarak alıcılar ile satıcıları eşleştirmek için kullanılabilir. Bu durumda, alıcı taraf satıcı tarafın menkul kıymete sahip olduğunu satıcı taraf ise alıcı tarafın yeteri kadar nakit paraya sahip olduğunu işlemden önce tespit edebilir Ancak bahsedilen bu kısım mevcut durumda piyasa girişimlerinin odak noktası değildir.[32]

[32] Mevcut piyasa girişimleri çoğunlukla işlem sonrası faaliyetlere odaklanmış durumdadır.

6. DLT UYGULAMALARININ OLASI ZORLUKLARI VE SINIRLAMALARI

DLT sisteminin bir önceki bölümde bahsedilen faydalara ulaşabilmesi için öncelikle olası birçok zorluğun üstesinden gelmesi gerekiyor. Bu zorlukların bazıları doğrudan teknolojinin kendisi ile ilgiliyken bazıları ise ağırlıklı olarak yönetim, gizlilik ve regülasyon konuları ile ilgilidir. Bu konular aşağıda ayrıntılı olarak ele alınmaktadır.

6.1 Teknolojik Konular

Ölçeklenebilirlik

Teknolojinin hızla gelişmekte olduğu günümüzde bazı firmalar hedefledikleri finansal faaliyetlerini gerçekleştirmek için DLT'yi kullanmaya başlamıştır. Bununla birlikte, menkul kıymetler piyasasında DLT sisteminin geniş ölçekte kullanılabilirliğine ilişkin somut bir örnek bulunmamaktadır. Bu nedenle, mevcut durumda belirli faaliyetler için kullanılmakta olan DLT sisteminin çok çeşitli araçların ve katılımcıların dâhil olduğu geniş bir ölçekte kullanılması bir takım problemlere neden olabilir. Çünkü teknolojinin fikir birliği algoritmaları gibi özelliklerle sağladığı düşük bekleme süresi gibi bazı avantajların, teknolojinin geniş bir ölçekte kullanılması durumunda bu algoritmaların çok fazla kaynak tüketmesi gibi nedenlerle dezavantaj olma potansiyeli bulunmaktadır.

Mevcut Sistemlerle ve Farklı Ağlarla Birlikte Çalışabilirlik

DLT sisteminin tüm piyasa faaliyetlerinde aynı anda kullanılması muhtemel görünmemektedir. Çünkü tüm piyasa katılımcıları yeni teknolojiyi kullanmayı seçmeyebilir veya mevcut piyasa altyapıları farklı blok zincirleri ile çalışmanın anında bir fayda sağlamayacağını düşünebilir. Yani adım adım senaryoda, DLT'nin mevcut piyasa altyapıları ve sistemleri ile en azından kısa ve orta vadede birlikte çalışması gerekecektir. Buna ek olarak farklı varlık türleri için ayrı blok zincirlerinin kullanılması ve bu zincirlerin birbirleriyle etkileşime girmesi de gerekebilecektir. Bu durumlar ise bir takım teknik sorunları ortaya çıkarmaktadır. Ayrıca bu durumlarda, DLT kullanımının mutabakat, takas ve takas öncesi işlemlerde sağlayabileceği faydalarının birçoğu, DLT piyasa katılımcıları ve altyapıları tarafından geniş ölçüde benimsenmediğinden sistemin bir bütün olarak çalışamaması nedeniyle azalabilir. Çünkü böyle bir durumda DLT kullanan ve kullanmayan sistemlerin hala bir biri ile DLT sistemi dışında farklı bir yöntem ile iletişim kurması gerekecek ve işlemlerin ağ dışına çıkmadan, anında tamamlanması mümkün olmayacaktır.

Merkez Bankası Parasının DLT Sistemine Entegre Edilebilirliği

İşlemlerin takasında teslim karşılığı ödeme (DVP) prensibini tam olarak sağlayabilmek için, varlık ve nakit bacaklarının aynı anda işleme tabi tutulması gerekmektedir. Bu durumda, yasal para birimleri DLT'ye kaydedilmediği sürece DLT

ve yasal para birimleri arasında bağlantıyı sağlayan bir köprü gerekecektir. Böylece de yine bir takım teknik ve yasal konular ortaya çıkmaktadır.

Başvuru Mekanizması

Mevcut tasarımda DLT sisteminde değiştirilemez paylaşılan kayıtlar oluşturulmaktadır. Başka bir deyişle onaylandıktan sonra işlemler değişmez olarak kabul edilir ve sistem tarafından bu işlemlerin değiştirilmesine veya iptal edilmesine izin verilmez. Bu bir taraftan, potansiyel bir fayda olarak görülebilir. Ancak diğer taraftan, hatalı işlemleri belirlemeye kimin yetkili olacağı, hangi zaman dilimine göre nasıl bir düzeltme mekanizması uygulanacağı gibi muhtemel hataların teknolojik ve yönetimsel olarak nasıl ele alınacağı sorununu ortaya çıkarmaktadır. Ayrıca DLT takas ve takas öncesi işlemlerin hızını potansiyel olarak artırabileceğinden düzeltme işlemleri için tasarlanacak başvuru mekanizmalarının da muhtemel hataları hızlı bir şekilde düzeltebilmesi gerekmektedir.

Pozisyon Netleştirme

Mevcut tasarımda DLT'de her işlem sıralı olarak brüt bir şekilde kaydedilmektedir. Bu şekildeki muhasebe yöntemi spot işlemler için uygun olmakla beraber türev işlemler için bazı sorunlar doğurabilir. Örneğin türev araç işlemleri için gerekli teminat miktarı net pozisyonlar üzerinden hesaplanmaktadır. Yani teknolojinin hâlihazırda çalıştığı yönteme değişiklikler getirilmediği sürece netleştirme olmaması türev araç işlemleri için teminat ve sermaye ihtiyacının artmasına sebep olacaktır.

Kredili Alım ve Açığa Satış

Mevcut durumda kredili alım piyasa katılımcılarına işlem yapılan varlıkları harici olarak finanse edebilme imkânı vermektedir. DLT sisteminde ise varlıklara sahip olunması işlem gerçekleştirebilmenin ön koşulu olduğundan bu tür işlemleri gerçekleştirebilmek mümkün olmayabilir. Aynı problem açığa satış işlemlerinde de geçerlidir.

6.2 Yönetim ve Gizlilik Konuları

Yönetim Çerçevesi

Menkul kıymet piyasasına uygulanması muhtemel DLT'nin, başlangıçta Bitcoin gibi sanal para birimleri için tasarlanan sınırlamasız blok zinciri sisteminin aksine verimlilik, güvenlik ve gizlilik amaçlarıyla sınırlamalı blok zinciri sistemi olması gerektiği değerlendirilmektedir. Bu şekildeki izin tabanlı sistemlerde yalnızca yetki verilen katılımcılar işlemleri doğrulayabilir ve işlemleri doğrulayan düğümlerin kimlik bilgileri ağın geri kalanı tarafından bilinir.

Sınırlamalı blok zincirinin izin tabanlı çerçevesi ise, katılımcıları onaylamak veya reddetmek için bir takım kuralları gerekli kılmaktadır. Bu kuralları tasarlarken düşünülmesi gereken faktörler ise minimum sermaye gerekliliğini, risk yönetim süreçlerini ve sistemin genel idaresini içerebilir. Kurallar tasarlanırken ayrıca sistemi

gereğinden fazla karmaşık hale getirme riskine rağmen birçok katılımcıyı kabul etme veya aşırı seçici davranarak ağın kapsamını sınırlama arasında bir denge bulunması gerekmektedir.

Bunlara ek olarak hem sınırlamalı hem de sınırlamasız sistemlerde katılımcılar arasındaki etkileşimleri yönetecek kurallar da gerekecektir. Bu kuralların ise birçok potansiyel karmaşık konuyu ele alması gerekir. Bu konuların örnekleri arasında ise katılımcıların yükümlülükleri, düzeltme mekanizmaları, dolandırıcılık ile mücadele yer almaktadır. Ayrıca ücretlendirme modeline ilişkin katılımcılar arasında bir anlaşmaya da ihtiyaç duyulmaktadır.

Dahası, yönetim çerçevesi özellikle regülatörler ve faaliyetlerinden sorumlu tutulacak kullanıcılar üzerinde netlik sağlamalıdır.

Gizlilik

DLT sisteminde tasarım gereği blok zincirine kaydedilen bilgiler ağın bütün katılımcılarına veya en azından izin verilen katılımcılara açıktır. Bu bilgi genellikle işlem tarihi ile hesaplarda tutulan nakit ve varlıkların bakiyesini içermektedir. Buna ek olarak, DLT'nin bazı durumlarda müşteri tanıma prosedürleri gereği müşterilerin özel bilgilerini saklamak ve paylaşmak için de kullanılması gerekmektedir. Bu durumda ise, teknolojinin doğasında olan blok zincirinin herkese açık yapısı ile blok zincirine kaydedilen bazı bilgilerin gizlilik ve mahremiyetini koruma gereksiniminin nasıl birleşebileceği problemi ortaya çıkmaktadır. Diğer taraftan isimler yerine özel anahtar gibi kripto tanımlayıcıların kullanılmasının bir miktar gizlilik sağladığı söylenebilir. Örneğin bir hesap sahibinin adı veya işlemdeki bir tarafın kesin kimliği ağdaki çoğu katılımcı tarafından bilinmeyebilir. Yine de, bu özel anahtarların çalışması dikkatle tasarlanmalı ve kontrol edilmelidir. Ayrıca katılımcıların niteliğine ve kapsamına bağlı olarak blok zinciri ağına farklı seviyelerde erişim gerekli olabilir.

6.3 Düzenleyici ve Yasal Konular

DLT'nin mevcut düzenleyici çerçeveye uyma kapasitesi, gelişimini sınırlayabilecek bir faktör olabilir. Uygulanması muhtemel önemli düzenlemeler ve DLT katılımcıları açısından bu düzenlemelerin yansımalarının ne şekilde olacağı bölüm 8' de daha ayrıntılı olarak ele alınmaktadır.

DLT'de tutulan kayıtların yasal olarak geçerliliği konusunun da dikkatlice incelenmesi gerekmektedir. Ayrıca DLT ağının denetlenmesi özellikle farklı düğümlerin farklı yargı alanları içerisinde yer alma ihtimalinden dolayı farklı gizlilik, iflas ve diğer gerekliliklere tabi olabileceğinden mevcut piyasa şirketlerini ve altyapılarını denetlemekten daha karmaşık olabilir.

7. ANA RİSKLER

Esas itibariyle DLT'nin menkul kıymet piyasalarına getirebileceği bazı potansiyel faydalar yukarıda belirtilen birtakım zorlukların giderilmesine bağlıdır. Ayrıca teknoloji ile ilgili bazı potansiyel riskler bulunmaktadır ve bunlar aşağıda ayrıntılı olarak tartışılmıştır. Bu risklerin bazıları DLT'ye özel olmakla beraber diğerleri mevcut piyasa altyapısında hâlihazırda mevcut olan ancak DLT'nin yaygın olarak kullanılması ile artma potansiyeli bulunan risklerdir.

7.1 Siber Risk, Dolandırıcılık ve Kara Para Aklama

Çalışmanın DLT'nin faydalarının vurgulandığı bölümlerinde de belirtildiği üzere blok zincirinin paylaşılan yapısı, mevcut sistemlerde geçerli olan tek bir noktayı hedef alan siber saldırının sistemin tamamını çalışamaz hale getirmesi riskini önemli ölçüde azaltmaktadır. Ancak bununla birlikte sistemdeki bir problemin daha geniş sonuçları olma riski de bulunmaktadır. Örneğin sisteme siber saldırı sonucu girmeyi başaran kişilerin yalnızca saldırı noktasında saklanan bilgilere değil blok zincirinin genelinde kayıtlı olan bilgilere erişebilme potansiyeli bulunmaktadır ki bu durum verilerin gizliliği ve bütünlüğü üzerinde çok olumsuz sonuçlar doğurabilir. Ayrıca, siber saldırı sonucu şifreleme teknikleri gibi teknolojinin kendisi ile ilgili yapıların ele geçirilmesi durumunda, farklı DLT ağlarının da benzer teknolojileri kullanma eğiliminde olması nedeniyle bulaşma riski saldırının tek bir DLT ağının ötesine geçmesine sebep olabilmektedir.

Genel/özel anahtarlar çalınması durumunda dolandırıcılık amacıyla hayali işlemler gerçekleştirmek için kullanılabilir. Yeterince sağlam bir yönetim çerçevesinin bulunmaması durumunda ise sahtekâr düğümler ağın bir kısmını kontrol altına alarak fikir birliği sürecini bozabilir. Benzer şekilde yeterli kontrollerin olmaması durumunda ise, mimaride yer alan genel/özel anahtar kullanımı işlem tarihi ile kimlik bilgileri gibi verileri gizlemeye imkân verdiğinden DLT kara para aklama ve terörün finansmanı faaliyetlerinde kullanılabilir.

7.2 Operasyonel Riskler

DLT kullanımı ile birlikte arka ofis süreçlerinin otomasyonun artması ve insan kaynaklı hataların azalacak olması nedenleriyle operasyonel risklerin azalması muhtemeldir. Ancak piyasa katılımcılarının süreçleri büyük ölçüde otomatik hale getirecek aynı sisteme güvenecek olması sistemdeki bir aksaklık veya arızanın çok büyük sonuçlara neden olması riskini ortaya çıkarmaktadır.

Benzer şekilde akıllı sözleşmelerin kullanılması kurumsal işlemleri otomatikleştirerek hata olasılığını azaltabilir. Ancak bununla birlikte kodlama hatası olması gibi durumlarda yeterli kontrollerin olmaması nedeniyle ilave riskler yaratabilir. Başka bir deyişle özet olarak DLT sisteminde hataların ortaya çıkma ihtimali daha düşük olabilir ancak etkilerinin yüksek olma potansiyeli bulunmaktadır.

7.3 Piyasa Oynaklığı ve Birbirine Bağlı Olma

Benzersiz bir referans sistemi vasıtasıyla katılımcılar ve varlık sınıfları arasında sağlanan otomatikleştirilmiş ve uyumlu süreçler sayesinde DLT sürü psikolojisine katkıda bulunabilir ve bu da stres zamanlarında piyasa oynaklığını artırabilir. Ayrıca DLT'nin piyasa katılımcılarının bir birine olan bağlılığını artıracak olması ve birbirleriyle etkileşim kurmalarını kolaylaştıracak olması piyasada yaşanan şokların yayılmasını da artıracaktır. Örneğin DLT sistemi ile sağlanan akıllı sözleşmeler ile işlem yapılması teminat tamamlama çağrılarının otomatik olarak tetiklenerek birbirini etkilemesine ve sistemde ciddi likidite oluşmasına neden olabilir.

Ayrıca DLT, nasıl ve kimin kullanacağına bağlı olarak piyasanın daha az düzenlenen bölümlerinde yoğunlaşma oluşması riskine neden olabilir. Örnek olarak DLT kullanarak bir noktadan diğerine gizli ödeme yapılmasını mümkün olabilir. Son olarak DLT, hantal işlem sonrası süreçler nedeniyle gelişemeyen piyasa faaliyetlerini destekleyebilir bu da finansal piyasalarda teknoloji ile ilgili yeni risklerin oluşmasına sebebiyet verebilir.

7.4 Adil Rekabet ve Düzgün İşleyen Piyasa

DLT kullanımı adil rekabete ilişkin birtakım sorunların ortaya çıkmasına neden olabilir. Örneğin DLT ağını destekleyenler yeni katılımcıların ağa dahil olmasına, ağa katılmaları ekonomik açıdan elverişsiz hale getirerek engel olabilir. Bu da hizmetlerin maliyetini ve kalitesini olumsuz etkileyebilecek tekel benzeri bir durumu ortaya çıkarabilir.

Rekabetçi blok zincirlerinin kurulmasının veya blok zincirleri arasında birlikte çalışılabilirliğin sağlanmasının zor olması menkul kıymet piyasalarının rekabetçi yapısını olumsuz etkileme potansiyeli taşımaktadır. Ayrıca yeterli kontroller yapılmadığı takdirde, ağın bazı katılımcıları ağ üzerinde kaydedilen diğer yatırımcıların işlem ve stok bilgileri gibi verileri piyasayı manipüle etmek amacıyla uygun olmayan şekilde kullanabilir. Başka bir deyişle blok zinciri ağının mahremiyet seviyesi ve güvenlik önlemleri ne kadar düşük olursa risklerde o kadar yüksek olmaktadır.

7.5 Diğer Riskler

DLT sistemi, risk yönetimi ve gözetimi perspektifinden bakıldığında olumsuz etkilere sahip olabilecek şifreleme tekniklerini kullandığından menkul kıymet piyasalarına bir miktar karmaşıklık getirebilir. Aslında, prensipte DLT, işlemlerin izlenebilirliğini ve menkul kıymet piyasalarındaki şeffaflığı artırmaktadır ancak işlemlerin şifrelenmesi en azından kısa vadede bilgilerin ayrıştırılması ve işlenmesini zor hale getirebilir ki bu da etkin bir şekilde denetim yapılmasını olumsuz etkileyebilir.

DLT sistemi ile ilgili bir başka risk ise yeni bir sisteme geçmenin belirsizliği ile ilgilidir. Operasyonel risk gibi bazı riskler DLT sistemine geçiş aşamasında artabilir. Ayrıca iki paralel sistemin aynı anda kullanılması kısa ve orta vadede finansal hizmet sunanlar ile kullanıcılara ek maliyetler getirebilir.

8. DÜZENLEYİCİ ÇERÇEVE ANALİZİ

Mevcut piyasa gelişmelerine uygun olarak DLT'nin öncelikle takas öncesi işlemler ve takas işlemleri gibi işlem sonrası faaliyetlerde uygulanacağı öngörüldüğünden çalışmanın bu bölümünde, menkul kıymet piyasalarına uygulandığında DLT'nin mevcut AB ve Türkiye düzenleyici çerçevesinde nasıl ele alınabileceğine yönelik analiz ortaya konulmaktadır. Ancak hemen belirmek gerekir ki bu bölümde yapılan analizin, teknolojinin halen gelişmekte olduğu ve uygulamalarının zaman içinde gelişebileceği göz önüne alındığında kapsamlı olmadığı değerlendirilebilir.

Ayrıca 2008 krizi sonrası dünyada sermaye piyasası altyapı kurumları olarak tanımlanan MKT'ler ve MSK'ların sistemik önemi artmıştır. Yatırım kuruluşu ve yatırımcılara bu kurumlar tarafından sağlanan hizmetlerin ise daha güvenli ve etkin şekilde yürütülmesi ihtiyacı hâsıl olmuş ve bu doğrultuda sektörde hızlı bir değişim gözlenmiştir. Avrupa gibi gelişmiş piyasalarda MKT ve MSK faaliyetlerini etkileyen ve etkilemesi beklenen yerel ve uluslararası düzenlemeler çıkmıştır. Bu düzenlemeler, yeniden oluşturulan uluslararası sektörel standartlar sermaye piyasası kurumlarının daha rekabetçi bir ortamda faaliyet göstermelerine ve sürekli değişen iş modellerine adapte olma çalışmalarına ağırlık vermelerine neden olmuştur.

Türk sermaye piyasası altyapı kurumları açısından bakıldığında ise, SPKn sermaye piyasalarına uluslararası standartların getirilmesinin önünü açmış ve altyapı kurumlarının görevlerinin yasal olarak düzenlenmesini sağlamıştır. Dünyada ise finansal altyapı faaliyetlerini doğrudan düzenlemesi bakımından bir ilk Avrupa Birliği Merkezi Saklama Kuruluşları Tüzüğü'dür ve burada (Central Securities Depositories Regulation, CSDR) MSK'lar bir menkul kıymet takas sistemi işleten (securities settlement system) ve bununla birlikte menkul kıymetlerin ilk kaydının yapılması (notary service) ve menkul kıymet hesaplarının en üst seviyede merkezi olarak tutulması (central maintenance service) faaliyetlerinden en az birini yerine getiren kurum olarak tanımlanmaktadır[33] (European Parliament & European Council, Mart 2012, 20).

Diğer taraftan Türkiye sermaye piyasası altyapı kurumları da küresel rekabetin giderek arttığı bir sektörde ayakta kalabilmek için ürettikleri hizmetlerin sadece Türk sermaye piyasası katılımcılarına yönelik değil uluslararası kurum ve yatırımcıların kullanımı için adapte edilebilir esneklikte olmasını amaçlamalıdır. Esas itibariyle de birkaç küçük eksiklik dışında[34] Türkiye sermaye piyasası altyapı kurumlarının CPSS-

[33] Netleştirme gibi takas öncesi işlemler dünyada bazı MSK'lar tarafından verilmekte ise de özellikle kriz sonrasında MSK'ların takas ve saklama sistemi dışında risk üstlenmesi sınırlandırılmakta ve takas öncesi kurumlar/MKT'ler ile MSK'ların faaliyetleri birbirinden ayrıştırılmaktadır.

[34] Türk sermaye piyasası altyapısının uluslararası endüstri standartlarına uyum konusundaki eksikliklerinden biri sermaye piyasasında merkezi saklama hizmetleri sağlayan birden fazla kurumun bulunmasıdır.

IOSCO Prensipleri, EMIR, CSDR vb. uluslararası düzenlemeler ve endüstri standartlarına tam uyum göstermektedir. Zira, her ne kadar ülkemiz kurumlarının yukarıda bahsi geçen düzenlemelere tam uyum göstermek konusunda hukuki bir zorunluluğu bulunmasa da gerek Türkiye'nin AB üyesi olma sürecinde bulunması gerekse bahsedilen düzenlemelerin Türk kurumlarını da dolaylı olarak etkileyecek olması bu duruma yol açmaktadır. Örneğin, EMIR ve CSDR gibi düzenlemelerdekilere benzer hükümler içermeyen bir mevzuat çerçevesinde faaliyet gösteren üçüncü ülke MKT'leri AB merkezli kurumlara hizmet verememe tehlikesi altındadır. Özellikle uluslararası işlemlerin büyüklüğü ve uluslararası finans merkezi olma hedefi dikkate alındığında, sadece Türk değil uluslararası işlem taraflarına da hizmet verilebilmesi son derece önemlidir. Bu doğrultuda, çalışmanın bu bölümü özellikle EMIR, SFD, CSDR gibi işlem sonrası faaliyetlerle ilgili temel AB mevzuatına odaklanmaktadır. MiFID, UCITS, AIFMD gibi diğer mevzuat konuları da bu bölümde tartışılmıştır.[35] Bu kapsamda çalışmanın bu bölümü takas öncesi işlemler, takas, saklama, raporlama ve diğer faaliyetler olarak organize edilmiştir.

8.1 Takas Öncesi İşlemler

AB'de takas öncesi işlem faaliyetleri EMIR ve MiFIR tarafından yönetilmektedir. EMIR OTC işlemlerin bazı türlerinin merkezi karşı taraf aracılığı ile tamamlanmasını, bazı türlerinin ise risk azaltma tekniklerine tabi tutulmasını gerekli kılmaktadır. MiFIR ise takas öncesi işlemler yükümlülüğünü düzenlenen piyasalara genişletmektedir.

EMIR'in 5 inci maddesi uyarınca, belirli standart OTC türev işlem türleri MKT yükümlülüğüne tabidir. MKT yükümlülüğüne tabi olmayan OTC işlemler içinse, EMIR'in 11 inci maddesi bu varlıkların operasyonel riskini ve karşı taraf kredi riskini ölçmek, izlemek ve hafifletmek için risk azaltma tekniklerine tabi olmasını öngörmektedir. 11 inci madde çift taraflı teminatlara ilişkin şartları içermektedir.

EMIR madde 2(3)'e göre takas öncesi işlemler, net yükümlülüklerin hesaplanması da dâhil olmak üzere pozisyonların tesis edilmesi ve bu pozisyonlardan kaynaklanan riskleri karşılamak için finansal araçların, nakit paranın veya her ikisinin de mevcut olduğundan emin olunması anlamına gelmektedir.

EMIR'in 2(1) inci maddesi MKT'yi, bir veya daha fazla finansal piyasada işlem gören sözleşmelerde karşı taraflar arasına kendisini yerleştirerek alıcıya karşı satıcı, satıcıya karşı alıcı rolünü üstlenen yetkilendirilmiş tüzel kişilik olarak tanımlamaktadır. MKT'ler sermaye yükümlülüğü, davranış kuralları, açık erişim kuralları ve raporlama gibi geniş bir yükümlülük kümesine uymak zorundadır. Ayrıca MKT'ler EMIR'in 39 uncu maddesinde belirtilen ayrımcılık ve taşınabilirlik yükümlülüklerine de uymak zorundadır. MiFIR 29 uncu maddesi MKT'lerin takas

35 Uygulanması muhtemel bağlayıcı düzenleyici gerekliliklere rağmen, CPMI-IOSCO gibi bazı ilkeler de mevcut piyasa altyapılarının yerini alması durumunda DLT'ye uygulanması gereken gerekliliklerle ilgili faydalı bilgiler sağlayabilir.

öncesi işlemler yükümlülüğünü düzenlenmiş piyasalarda işlem gören türev araçlara kadar genişletmektedir.

Olası Senaryolar

Yukarıda belirtilen düzenlemelere dayanarak takas öncesi işlemler faaliyetini sunmak için DLT sistemi kurmak isteyen piyasa katılımcıları ilgili enstrüman türüne göre farklı gereksinimlere uymak zorunda kalacaklardır. Aşağıda olası senaryolar ve bu senaryoların DLT sistemi için yasal gereklilikler açısından ne ifade edeceği incelenmektedir.[36]

Senaryo 1: DLT sisteminde OTC türev işlemlerin takas öncesi faaliyetlerinin gerçekleştirilmesi

MKT yükümlülüğüne tabi olunması

Eğer piyasa katılımcıları tarafından MKT yükümlülüğüne tabi OTC işlemlerin takas öncesi faaliyetlerini gerçekleştirmek için DLT ağı kurulacaksa, bu DLT ağı EMIR ve diğer düzenlemeler tarafından belirlenen şartlara uymak zorunda olacaktır. Bu özellikle MKT'nin hala gerekli olacağı anlamına gelmektedir. Farklı düzeylerde fayda, maliyet ve risk taşıyabilecek bu gereksinimlere uymak için farklı çözümler planlanabilir. Örneğin bu çözümler mevcut bir MKT ile anlaşma imzalanması veya MKT olmak için yetki başvurusu yapabilecek yeni bir tüzel kişiliğin kurulması olarak sayılabilir.[37]

MKT yükümlülüğüne tabi olunmaması

EMIR'in 11 inci maddesi MKT kullanılmayan OTC türev araç sözleşmelerinin finansal ve finansal olmayan karşı taraflarına belirli yükümlülükler getirmektedir. Finansal ve finansal olmayan karşı taraflar, operasyonel risk ile karşı taraf kredi riskini ölçmek, izlemek ve hafifletmek için en azından aşağıda belirtilenleri içeren prosedürlerin veya anlaşmaların mevcut olmasını sağlamalıdır:

- Mevcut olduğunda elektronik olarak, ilgili OTC türev sözleşmesinin koşullarının zamanında teyidi,

- İlgili riski yönetmek, sözleşmelerin değerini izlemek ve taraflar arasındaki anlaşmazlıkları erkenden tespit ederek çözebilmek için esnek ve denetlenebilir süreçler.

Ayrıca EMIR'in 11 inci maddesi karşı taraflar arasında teminatın değiştirilmesi ile ilgili gereklilikleri de içermektedir. Bu doğrultuda, teminatın da, MKT üzerinden gerçekleştirilmeyen OTC türev işlemlerinde DLT'nin nasıl uygulanabileceği tasarlanırken dikkate alınması gerekecektir. Sonuç olarak MKT yükümlülüğüne tabi olmayan OTC türev işlemlerinde DLT kullanılacak olması durumunda sistemin,

[36]Bölüm 5.4'te vurgulandığı gibi, DLT türev araçlar konusunda sınırlı sağlayabilir.

[37] Aynı durum MKT yükümlülüğüne tabi olmayan ancak işlemleri MKT'ler tarafından gönüllü olarak gerçekleştiren işlemler için de geçerlidir.

finansal ve finansal olmayan karşı taraflara risk azaltma tekniklerini kullanmaya ve karşılıklı teminat yükümlülüğünü yerine getirmeye imkân verecek şekilde tasarlanması gerekmektedir.

Senaryo 2: Düzenlenmiş Piyasalarda İşlem Gören Türev Araçların Takas Öncesi İşlerinde DLT Kullanılması

MiFIR'in 29 uncu maddesine göre, borsada işlem gören türev işlemlerin takas öncesi işlemleri EMIR tarafından tanımlandığı gibi MKT üzerinden gerçekleştirilmelidir. Buna göre, eğer piyasa katılımcıları tarafından düzenlenmiş piyasalarda işlem gören türev araçların takas öncesi işlemlerini gerçekleştirmek için DLT kullanılması durumunda düzenlemelere uymak için MKT'ye hala ihtiyaç duyalacaktır.

Senaryo 3: Diğer Varlık Türlerinin Takas Öncesi İşlemlerinde DLT Kullanılması

Bazı MKT'ler ve takas kurumları gibi diğer piyasa altyapı kuruluşları tarafından türev araç dışındaki varlıklara ilişkin takas öncesi işlemler de gerçekleştirilmektedir. Bu varlıklara ilişkin takas öncesi işlerin MKT tarafından gerçekleştirilmesi durumunda izin ve sermaye gerekliliği gibi kurallar açısından EMIR ve diğer düzenlemelere uyulmalıdır. Bu varlıklara ilişkin bahse konu işlemlerin MKT dışında başka kuruluşlar tarafından gerçekleştirilmesi durumunda ise AB düzeyinde herhangi bir kural bulunmamaktadır.

8.2 Takas Faaliyetleri

Takas faaliyetleri temel olarak CSDR ve SFD düzenlemeleri tarafından yönetilmektedir. Bu düzenlemelerden CSDR'nin amacı takas döngüsünün ve takas disiplininin belirli yönlerini uyumlaştırarak AB genelinde menkul kıymet takas sistemi işleten MSK'lere yönelik ortak gereksinimleri belirlemektir. Ayrıca CSDR, AB'de sınır ötesi takas için düzenleyici ve operasyonel koşulları geliştirmektedir. Bu ise işlem sonrası faaliyetlerde kilit rol oynamaktadır. Belirli bir CSDR hükmünde aksi belirtilmediği sürece CSDR'nin, MSK faaliyetleri ile MiFID tarafından tanımlanan tüm finansal araçların takas işlemlerinin tamamlanmasında geçerli olduğu söylenebilir.

Öte yandan SFD, ödeme ve menkul kıymet takas sistemine katılım ile ilişkili sistemik riski ve bu tür sisteme katılan bir kişinin iflas etmesi ile ilgili riski azaltmayı amaçlamaktadır. Bu nedenle SFD, menkul kıymet takas sistemlerinin yanı sıra sistemdeki herhangi bir katılımcıya ve katılımla bağlantılı teminata yönelik olarak da uygulanmaktadır.

Temel Şartlar

Avrupa Parlamentosu tarafından sermaye piyasası altyapı kurumlarına yönelik G20 kararları paralelinde kabul edilen CSDR'nin, muhtemel bir DLT sisteminde önemli etkileri olacağı değerlendirilmektedir. Çünkü menkul kıymet ve nakit

borçlarının kapatılması ve bunlara bağlı hesap hareketlerini kapsayan alım-satım işleminin sonuçlandırılma aşamasını ifade eden takas işlemin DLT sistemi üzerinden gerçekleştirilebilmesi söz konusudur. Hali hazırda ise finansal araç ve nakit MSK'lar tarafından yönetilen takas sistemi üzerinden el değiştirmektedir. Bu nedenle takas işlemlerinde kullanılması muhtemel DLT sistemine ilişkin senaryo analizi yapabilmek açısından menkul kıymet takas sistemi, menkul kıymetlerin ilk kaydının yapılması ve menkul kıymet hesaplarının merkezi olarak tutulmasına ilişkin düzenlemeleri içeren CSDR'nin ilgili maddelerinin incelenmesinde fayda görülmektedir.

Bu bağlamda, CSDR'nin 3 üncü maddesinin birinci fıkrasına göre, işlem gören menkul kıymetlerin ihraççısı söz konusu menkul kıymetlerin kaydi olarak temsil edilmesini sağlamalıdır. Yine aynı düzenlemede kaydi sistemin nasıl sağlanacağına ilişkin herhangi bir yöntem belirtilmemektedir.

CSDR'nin 3(2) maddesine göre ise, devredilebilir menkul kıymetlerde bir işlem gerçekleştiğinde ilgili menkul kıymetlerin MSK'de kaydi olarak kaydedilmesi öngörülmektedir. Transfer edilebilir menkul kıymetlerin 2002/47 / EC sayılı Direktifin 2(1) maddesinin (a) bendinde tanımlandığı gibi mali teminat olarak devredilmesi durumunda ise söz konusu menkul kıymetlerin daha önceden kaydileştirilmemişse MSK'de kaydileştirilmesi gerekmektedir.

CSDR'nin 5 inci maddesinde menkul kıymet takas sistemindeki herhangi bir katılımcının söz konusu işlemleri planlanan takas gününde yapmasını öngörmektedir. Devredilebilir menkul kıymetlerdeki işlemlere ilişkin olarak, planlanan takas tarihi en geç işlemin gerçekleşmesinden sonraki ikinci iş günüdür.

CSDR'nin 6 ncı maddesi uyarınca MSK tarafından, faaliyette bulunulan her bir menkul kıymet takas sistemi için işlemlerin takasının planlanan tarihte gerçekleştirilmesini ve söz konusu tarihe kadar katılımcıların karşı taraf ve likidite risklerinin minimuma indirilmesini kolaylaştıracak prosedürler oluşturulmalıdır. 7 nci madde ise MSK'nin gerçekleşmeyen takasları izlemek için sistem kurmasını ve bu takas başarısızlıklarının giderilmesi için prosedürler oluşturmasını içermektedir.

CDSR'nin 9 uncu maddesine göre, takası menkul kıymet takas sistemlerinin dışında gerçekleşen işlemlerin toplam hacmi üçer aylık dönemlerde yetkili makamlara raporlanmalıdır.

CSDR'nin 18(2) maddesine göre menkul kıymet takas sistemleri MSK olarak görev yapan merkez bankaları da dâhil olmak üzere sadece yetkili MSK'ler tarafından işletilebilir. MSK'ler ise yetkili makamlar tarafından yetkilendirilmeli ve denetlenmelidir. Ayrıca MSK'ler sermaye ve organizasyon gerekliliklerini de içeren geniş bir gereklilik kümesine uymak zorundadır.

CSDR'nin 2 nci maddesinde ise takas içselleştiricisi menkul kıymet takas sistemi dışında takas emirlerini müşteri namına veya kendi adına yerine getiren yatırım kuruluşu gibi yetkili şirketler olarak tanımlanmaktadır.

Konu ile diğer bir düzenleme olan SFD'nin 3 üncü maddesinde de, virman talimatları ve netleştirmenin yasal olarak uygulanabilir olması ve üçüncü taraflar üzerinde bağlayıcı olması gerektiği belirtilmektedir. Ayrıca aynı düzenlemenin 9 uncu maddesi ise, teminat sahibi kişilerin haklarının, sağlayıcının iflasının etkilerinden yalıtılmasını öngörmektedir.

Takas Sistemine İlişkin Olası Senaryolar

Senaryo 1: Ev Sahibi Üye Ülke Tarafından Menkul Kıymet Takas Sistemi Olarak Belirlenmeyen Bir DLT Ağı Aracılığı İle İşlemlerin Takasının Gerçekleştirilmesi

Bu senaryoda DLT ağı bir menkul kıymet takas sistemi olarak belirlenmediğinden DLT sistemin MSK olarak nitelendirilmesi mümkün değildir. Dolayısıyla söz konusu sistem SFD düzenlemesine de tabi değildir.

Senaryo 1.1: DLT ağı, CSDR kapsamında takas içselleştiricisi olarak hareket etmiyor

DLT ağı sisteminde, CSDR kapsamına girmeyen ve bir MSK veya MSK olarak hareket eden merkez bankası tarafından işletilen menkul kıymet takas sistemine potansiyel olarak yerleştirilemeyen menkul kıymetlerin takasını gerçekleştirilebilir. Böyle bir durumda, DLT ağı CSDR kapsamında bir takas içselleştiricisi olarak davranmamaktadır ve bu nedenle yukarıda açıklanan raporlama gereksinimlerine de tabi değildir.

Senaryo 1.2: DLT ağı, CSDR kapsamında takas içselleştiricisi olarak hareket ediyor

DLT sistemi, takas içselleştiricisi olarak vasıflandırılmışsa, ilgili raporlama gerekliliklerine uymalıdır. Takas, bir menkul kıymet takas sisteminin dışında gerçekleştiğinde yani içselleştirilmiş takas durumda, CSDR takas içselleştiricileri için raporlama gerekliliklerini belirtmektedir. Dolayısıyla, DLT sistemi tarafından içselleştirilmiş takas kullanılması durumunda , ilgili menkul kıymetin CSDR'nin 9 uncu maddesinin kapsamına girmesi şartıyla CSDR'nin 9 uncu maddesinde belirtilen raporlama yükümlülüklerine de uyması gerekir. Bu senaryo ayrıca, DLT ağının MSK ile açılan hesaplarla doğrudan veya DLT ağının MSK tarafından işletilen menkul kıymet takas sisteminde katılımcı olduğu şekilde dolaylı olarak bağlantı kurmaya ihtiyacı olacağını ifade etmektedir. DLT ağının MSK tarafından işletilen menkul kıymet takas sisteminde katılımcı olması durumunda ise CSDR'de belirtilen katılım ve mutabakat şartlarına uyması gerekmektedir.

Senaryo 2: DLT Ağı, Menkul Kıymet Takas Sistemi Olarak Tasarlandı

DLT ağının menkul kıymet takas sistemi olarak tasarlanması durumda, söz konusu sistem için SFD şartları geçerli olacaktır. Böylece de SFD'nin 2 nci maddesine göre sisteme katılanlar ile resmi bir anlaşma yapılması ve sistem operatörünün belirlenmesi gerekecektir. CDSR'ye göre ise bu operatör CSDR şartlarını taşıyan bir

MSK olmalıdır. Yani bu MSK'nin minimum sermaye gerekliliği, iş yapış kuralları ve ihtiyati kurallar gibi CSDR gerekliliklerine uyması gerekmektedir.

8.3 Menkul Kıymetlerin Saklanması ve Kayıt Altına Alınması

Menkul kıymetlerin saklanması ve mülkiyetinin kayıt altına alınması için AB düzeyinde uyumlaştırılmış bir tanım bulunmamaktadır ve bu görevler saklama bankaları ve MSK'ler gibi geniş bir uygulama yelpazesi bulunan şirketler tarafından gerçekleştirilmektedir. Kurallar ayrıca, kayıt tutmanın ihraççı seviyesinde mi yoksa yatırımcı seviyesinde mi uygulandığına da bağlıdır.

Göz önüne alınması gereken diğer önemli bir husus ise menkul kıymetler için geçerli olan mevzuatın ve menkul kıymetlere eklenen hakların AB düzeyinde uyumlaştırılmamış olmasıdır. Yani menkul kıymetlerin ihraç edilmesine ve menkul kıymetlere eklenen haklara ilişkin hususlar ulusal düzenlemeler ile belirlenmektedir.

Ayrıca ulusal yasalar menkul kıymetin, bağlı bulunduğu yerin veya kayıtlarının tutulduğu yerin yasaları tarafından yönetilmesini sağlayabilir. DLT sisteminde ise, menkul kıymetlerin ve kayıtlarının tutulduğu yerlerin çok net olmadığı ifade edilebilir. Ek olarak, menkul kıymetlerin sahipliğinin transferi ile ilgili işlemlerde takas kesinliğinin nasıl sağlandığı ise diğer bir önemli hususdur.

Senaryo 1: İhraççı Düzeyinde Kayıt Tutulması

Sahiplik kayıtlarının ihraççı seviyesinde tutulması için, kurallar Ulusal Şirketler Hukukuna bağlı olacaktır. Bu nedenle, DLT'nin bu bağlamda kullanılabilirliğini belirlemek için ülke düzeyinde Şirketler Hukukunun değerlendirilmesi gerekmektedir. Örneğin Almanya'da medeni hukuk kurallarına uygun olarak menkul kıymet tesis edilebilmesi için ihraççının fiziki bir sertifika oluşturması gerekmektedir ve bu Almanya'da DLT ile menkul kıymetlerin tam olarak dijitalleşmesini engelleyebilecek bir husus olarak öne çıkmaktadır.

Bu bağlamda, konunun bütünlüğünü sağlamanın gerekli olduğunu vurgulamak oldukça önemlidir. Ayrıca CSDR'nin 37 nci maddesi uyarınca, ihraç edilen menkul kıymet sayısı ile katılımcıların menkul kıymet hesaplarında kayıtlı olan menkul kıymet sayısının eşit olduğunu doğrulamak için mutabakat önlemleri alınmalıdır.

Senaryo 2: Yatırımcı Düzeyinde Kayıt Tutulması

Sahiplik kayıtlarının yatırımcı düzeyinde tutulmasına ilişkin kurallar MiFID, UCITS ve AIFMD gibi çeşitli sektörel düzenlemelerde değişiklik göstermektedir**.** Özellikler UCITS ve AIFMD bağlamında, saklanan fonların ve varlıkların güvenli bir şekilde muhafaza edilmesinden saklayıcılar sorumludur. Bu nedenle, DLT sisteminin UCITS ve AIFMD kapsamında kullanılmak istenilmesi durumunda düzenlemelere uymak için hala bir saklayıcıya ihtiyaç duyulacaktır.

8.4 Düzenleyici Raporlama Faaliyetleri

MiFID, EMIR ve SFTR gibi birkaç mevzuat piyasa katılımcılarının yetkili makamlara veya veri depolama kuruluşları gibi üçüncü taraflara raporlama yapmalarını zorunlu kılmaktadır. Örneğin EMIR kapsamında, takası MKT üzerinden gerçekleştirilen ve gerçekleştirilmeyen türev sözleşmelerinin bilgilerinin veri depolama kuruluşuna bildirilmesini gerekmektedir. SFTR uyarınca ise menkul kıymet finansman işlemleri için benzer raporlama yükümlülükleri bulunmaktadır. Veri depolama kuruluşları ESMA tarafından denetlenen ve geniş bir kurallar dizisine uymak zorunda olan tüzel kişilerdir. Özellikle EMIR bu kuruluşlar için sıkı operasyonel, kayıt tutma ve veri yönetimi şartlar uygulamaktadır. Bu kapsamda, piyasa katılımcıları tarafından veri depolama kuruluşları ile aynı işlevi yerine getirmek amacıyla DLT ağı kurulmak istenilmesi durumunda EMIR'ın kurallarına uymak zorunda olan bir veri deposuna hala ihtiyaç duyulacaktır.

8.5 Diğer Faaliyetler

DLT, daha önce tartışılanlar dışındaki diğer ihraç hizmet türleri ve kitle fonlaması[38] gibi menkul kıymetler piyasasındaki diğer faaliyetler için de potansiyel olarak kullanılabilir.

[38] Kitle fonlaması platformlarında DLT kullanımının faydası şeffaflığın sağlanması olarak ifade edilebilir.

9. GENEL DEĞERLENDİRME ve SONUÇ

Teknoloji dünyasında meydana gelen gelişmeler hayatın birçok alanını olduğu gibi finansal hizmetler endüstrisini de etkilemekte ve yeniden şekillenmesine neden olmaktadır. Bilgi işlem gücünün artması; verilerin toplanması, işlenmesi ve depolanmasının maliyetinin düşmesi, erişilebilir veri ve veri kaynaklarının üssel olarak artması, verilerin paylaşılabileceği ve uygulamaların geliştirilebileceği altyapı ve platformların oluşması gibi faktörler FinTek kategorilerinin ortaya çıkmasına katkıda bulunmuştur.

Bu çalışmada da açıklandığı üzere FinTek, finans ve teknolojinin kesişim noktasında yer almakta ve finansal hizmetler endüstrisinde bir takım yıkıcı etkiler oluşturmaktadır. Öyle ki FinTek'lerin ortaya çıkması ve gelişmesiyle birlikte artık ihraççılar, yatırımcılar ve aracılar, geçmişten çok farklı yollarla iletişim kurmakta, araştırma yapmakta, sosyalleşmekte ve işbirliği yapmaktadır. Zira günümüzde yatırımcılar; sosyal alım satım platformlarında ve melek yatırımcı sitelerinde diğer yatırımcıları takip etmekte, mevcut piyasa verisi sayesinde yapay zekâ ve sosyal medya analizleri ile de menkul kıymet alım satımı ve yatırım kararı verme konularında analiz yapmaktadır. Ayrıca kitle fonlaması platformları internet ortamında projelere katılımcı finansman desteği sağlanmasına aracılık etmekte, denkler arası borçlanma platformları kredi satmakta veya satılmasına aracılık etmekte, robot-tavsiye uygulamaları otomatikleştirilmiş yatırım tavsiyeleri sunmakta ve sosyal alım-satım platformları bir sosyal ağ aracılığı ile yatırım hizmetleri sunmaktadır.

Ayrıca finansal sistemi çeşitli kanallardan etkileyen FinTek sayesinde finansal sistemin gelişmediği ülkelerde tabana yayılma artarken geleneksel kaynaklardan finansman sağlama imkânı bulamayan gerçek ve tüzel kişiler de yeni aracılardan kaynak edinme imkânına kavuşabilmektedir. Diğer taraftan, bu durum FinTek şirketlerinin rekabeti artırarak maliyet avantajı sağlama ve etkinliği artırma potansiyeli olduğunu göstermektedir.

FinTek sektörünün her geçen gün büyümesi ve finansal hizmetler endüstrisini dönüştürme potansiyelinin artması ise, finansal hizmetler endüstrisinin geleceği için etkili regülasyonlara olan ihtiyacı artırmaktadır. Regülatörler açısından ise hem FinTek'lerin gelişimine katkı sağlayacak hem de finansal sistemi güvence altına alacak şekilde FinTek sektörünün düzenlenmesi gerekmektedir. Çünkü düzenlemeler sayesinde aracılık faaliyetlerinde denkler arası borçlanma veya kitle fonlaması gibi alternatif yöntemlere bir miktar geçiş olması ve daha birçok inovatif iş modeli mümkün hale gelebilmektedir. Bu bağlamda, genel olarak regülatörlerin FinTek'lere yaklaşımının temel özellikleri;

- FinTek şirketleri için inovasyonu sağlayacak "sanal ortam" yaratılması.
- Düzenleyici kurumlar ve yurtdışı muhatapları arasında ortaklık kurulması.
- Düzenleyici kurumlar ve FinTek liderleri arasında inovasyon konusundaki problemleri ve çözümlerini belirlemek için uyumun sağlanması.

– FinTek inovasyonlarının büyümesini sürdürmek, rekabeti korumak ve sonuçta tüketicilere fayda sağlamak için FinTek'lere yönelik devlet desteğinin artırılması.

olmalıdır.

Öte yandan FinTek kategorilerinden bazılarının özellikle sermaye piyasalarında, belirli iş modelleri üzerinde yıkıcı etki oluşturma potansiyeli bulunmaktadır. Finansal aktörler arasında veri işleme ve paylaşma eylemlerini kolaylaştırmak için fikir birliği protokolleri ile her güncelleme hakkında mutabakat sağlanan dağıtılmış veri tabanı sistemini ifade eden DLT ise bu alanda yıkıcı etkilere sahip olma anlamında öne çıkmaktadır. Bilgisayar biliminin ve kriptografinin çeşitli alanlarından kavramlar, bu sistemi gerçekleştirebilmek için kullanılmaktadır.

Finansal piyasalar, menkul kıymet ihraççısının işi ile doğrudan ilgili olmayan operasyonel ve karşı taraf riski gibi riskleri önlemek için yasal anlaşmalar ve düzenlenmiş usuller aracılığı ile karşılıklı güven veren kurumların bir ağı olarak zaman içinde gelişmiştir ve bu piyasada hemen hemen her kurum, düzenleyici kurumların denetimi ve gözetimi altındaki hesap verme yükümlülüğü bulunan yetkilendirilmiş karşı taraflarla işlem gerçekleştirmektedir. Bitcoin[39] ağının amaçları için çok önemli olan, piyasa katılımcıları için takma ad kullanılması, sistemin denetlenemez olması, zincirin dünyanın her yerinden herkes tarafından erişilebilir olması ve gerçekleşen yasadışı işlemlerin iptal edilememesi gibi özellikler de finansal piyasalar için geçerli değildir. Ayrıca birbirleri ile veri paylaşmak isteyen finansal kurumlar arasında oluşturulan bir blok zinciri uygulamasında zincirin kontrolünün katılımcıların hepsine bırakılması genellikle pek uygun değildir. Bu doğrultuda öncelikle takas öncesi işlemler ve takas işlemleri gibi işlem sonrası faaliyetlerde uygulanacağı öngörülen DLT'nin okuma ve yazma izinleri tamamen herkese açık olacak şekilde veya herkes okuma iznine sahipken sadece belirli düğümlerin yazma izni olacak şekilde yetkilerin ayarlanabildiği sınırlamalı blok zinciri mimarisinde olması gerektiği değerlendirilmektedir. Çünkü sınırlamalı blok zincirinde, katılımcıların kimliği en azından yönetim organı tarafından bilinmekte ve bu da haksızlığa yol açabilecek herhangi bir yanlış davranışın cezalandırılabileceğini ifade etmektedir. Ayrıca sınırlamalı blok zinciri katılımcıların zincirde gerçekleştirdikleri işlemlerin yanı sıra uygulama dışında gerçekleştirdikleri işlemler açısından da uymaları gereken kurallar bulunması nedeniyle sınırlamalı blok zincirleri, geleneksel finans sisteminde yüksek düzeyde olan şeffaflık ve hesap verilebilirliğin bir örneğini oluşturmaktadır.

Blok zinciri uygulamalarının ağa katılım açısından sahip oldukları çeşitli özellikler, ağın verimliliğini de dolaylı olarak etkilemektedir. Her katılımcının blok zincirinin korunması için fazla kaynak ayırması yerine blok zincirini koruma

[39] İnternetin ilk yıllarında e-posta'nın internet için bir katalizör görevi görmesine benzer şekilde, sanal para birimleri de blok zincirleri için şu anda katalizör görevi görmektedir. Bu nedenle DLT sisteminin sürekli olarak Bitcoin ve sanal para birimleriyle anılması normaldir.

yükümlülüğü, yasalara karşı davranışının cezalandırılacağını bildiğinden iyi niyet kuralları çerçevesinde hareket edecek katılımcılara bırakılabilir. Bu şekilde, sınırlı blok zinciri uygulamalarında doğrulama işlemi tüm katılımcılar için maliyetli hale getirilmez ancak saldırganlar için sistemi ele geçirmek hala maliyetli kalmış olur. Bu kapsamda, sermaye piyasalarında kullanılacak sınırlamalı blok zinciri mimarisinde yer alacak fikir birliği algoritmasının PoS tabanlı olması gerektiği değerlendirilmektedir. Ayrıca sistemde kullanılan doğrulama kuralları ise hem ekonomik teşviklerden hem de kriptografik güvenlik özelliklerinden yararlanarak siber esneklik ve verimlilik arasındaki dengede tatminkâr bir uzlaşma bulmalıdır.

Sermaye piyasalarında önerilen şekilde sınırlamalı DLT kullanımı ile aracıların sayılarının azaltılması ve mutabakat sürecinin daha verimli hale getirilmesi suretiyle bazı finansal işlemlerin takas ve takas öncesi işlemler sürecinin hızlandırılması sağlanabilir. Bu doğrultuda söz konusu sistemin aşağıda sıralanan faydaları sağlayacağı değerlendirilmektedir.

-Takas öncesi işlemler ve takas işlemleri tek bir adımda neredeyse anlık olarak gerçekleştirilmesi karşı taraf riskinin ve teminat gönderme gereksinimin azalmasını sağlar.

-Sistemin paylaşılan yapısı ve sistemde fikir birliği algoritmalarının kullanılması mutabakatlaşmaya ilişkin süreçlerin da daha verimli hale gelmesini sağlar.

-Sistem dijital menkul kıymetleri ihraç etmek, sahipliklerini izlemek ve ihraç ile ilgili hizmetleri desteklemeye yardımcı olmak için kullanılabilir.

-Tek bir kaynaktan edinilen bilgiyle kıyaslandığında mevcut bilgi içeriğinin kapsamının genişletilmesi ve bu bilgiye daha hızlı erişim imkânı sağlanması suretiyle; raporlama, risk yönetimi ve denetim amaçlı verilerin toplanması süreci verimli hale getirilebilir.

-Sistemde her kayıt geçmiş versiyonları ile görülebilmektedir. Bu özellik gerekli önlemlerin alınması koşuluyla, raporlama görevlilerine, risk yöneticilerine ve düzenleyicilere kolaylık sağlayabilir.

-Sistemin spot işlemlerde karşı taraf riskini azaltma hatta ortadan kaldırma potansiyeli bulunmaktadır. Böylece piyasa katılımcıların, belirli işlemler için daha kısa süre daha az teminat göndermesi veya hiç teminat göndermemesi mümkün olabilir. Ancak hâlihazırda spot işlemlerin büyük bir kısmı teminatsız olarak yapılmaktadır ki bu da DLT'nin bu alandaki faydasını sınırlandırmaktadır.

-Genel bir maliyet düşüşü ise, sistemin öne çıkan en önemli faydalarından biridir. İşlem sonrası faaliyetlerde, mevcut durumda manuel olarak yapılan bazı işler DLT kullanımı ile otomatikleştirerek orta ve arka ofis süreçlerini hızlandırabilir ve dolayısıyla maliyetler azaltılabilir. Aynı durum raporlama ve izleme işlevleri için de geçerlidir.

- Sistem sayesinde şirket düzeyinde tutulan münferit kayıtların yerine, kayıtların sisteme dağıtılmasıyla mutabakatlaşma maliyetini azaltabilir veya hatta ortadan kaldırabilir.

- Sistemin dağıtık mimaride olması sistemin çalışamaz duruma gelmesini oldukça zorlaştırmakta ve bu da DLT kullanımı ile maliyeti oldukça yüksek olan iş sürekliliği planlarına olan ihtiyacı azaltmaktadır.

Öte yandan, bu teknoloji geçiş aşamasında olduğundan henüz farklı altyapılarla birlikte çalışabilirliğe ilişkin fikir birliği ve mevcut düzenlemelere uyum konusunda ülke ve sektörlerde standart bulunmamaktadır. Ayrıca DLT sistemlerinin eski süreçler ve sistemlerle birlikte nasıl işleyebileceği, olası performans ve güvenlik problemleri, görünmeyen maliyetler ve en önemlisi de yasal uyum çerçevesi mevcut durumda belirsizdir.

Sonuç olarak, halen gelişimine devam eden bir inovasyon alanı olan söz konusu sistemin açıklanan olası faydalarına ulaşılabilmesi için uygulamada öncelikle teknoloji ile ilgili siber risk, dolandırıcılık ve kara para aklama gibi bazı potansiyel risklerin ve yönetim, gizlilik, FinTek regülasyonu, ölçeklenebilirlik, mevcut sistemlerle ve farklı ağlarla birlikte çalışabilirlik gibi önceki bölümlerde açıklanan muhtemel birçok zorluğun üstesinden gelinmesi gerekmektedir. Bununla birlikte, temelinde dağıtılmış defter mantığında çalışan yeni nesil işlem doğrulama mekanizması olan DLT sisteminin 5-10 yıl içerisinde geleneksel sistemlerin yerini alabileceği ve finans, fon transferi, ödemeler, sermaye piyasaları, varlık yönetimi, e-ticaret, politika, sanat ve daha birçok alanda pratik uygulamaları olacağı değerlendirilmektedir. Bu bağlamda, sermaye piyasaları özelinde çalışmanın önceki bölümlerinde önerilen uygulama senaryoları önemli olmaktadır.

KAYNAKÇA

1. Adair, John. Yenilikçi Liderlik - Takım Üretkenliğinin Organizasyonu ve Fikirlerin Hasadı, 1. Baskı, Babıali Kültür Yayıncılığı, İstanbul 2008.
2. Uzkurt, Cevahir. Pazarlamada Değer Yaratma Aracı Olarak Yenilik Yönetimi ve Yenilikçi Örgüt Kültürü, Beta Basım Yayım Dağıtım A.Ş. İstanbul 2008.
3. Yavuz, Çağla. İşletmelerde İnovasyon (yenilikçilik) Stratejileri ve Örgütsel performans İlişkisinin Çanakkale Seramik A.Ş. İşletmesi Örneğinde Boylam Analizi Yöntemiyle İncelenmesine Dönük Bir Araştırma, Çanakkale Onsekiz Mart Üniversitesi Yüksek Lisans Tezi, Çanakkale
4. Özgenç, Ali. İnovasyonun Adında Kalmak, Capital Dergisi, 2009, 254.
5. OECD - Oslo Manual: Proposed Guidelines for Collecting and Interpreting Technological Innovation Data, Paris 2005.
6. Schumpeter, Joseph. (1943). Capitalism, Socialism and Democracy, New York: Harper.
7. Güneş, Serkan. Değer Yaratma Bağlamında Güncel Dört Yenilik Modeli, Sanat ve Tasarım Dergisi, Sayı:7
8. Teece, David., Coleman, Mary. (1998). The Meaning of Monopoly: Antitrust Analysis in High Technology Industries, The Antitrust Bulletin, 93:801-859.
9. Bower, J. L., & Christensen, C. M. (Ocak-Şubat 1995). Disruptive Technologies: Catching the Wave. Harvard Business Review
10. Reagan, J. L. (2014, Şubat). Predicting Disruptive Innovation: Which Factors Determine Success? . Tez . New York, ABD: B.A. State University
11. Özçakmak, Fuat (2016, Ocak). Yıkıcı Teknolojilerin Tespit Edilmesi.
12. Schumpeter, Joseph. (1943). Capitalism, Socialism and Democracy, New York: Harper.
13. Clayton M. Christensen, Michael B. Horn, and Heather Staker (2013): Is K–12 Blended Learning Disruptive? An introduction to the theory of hybrids.
14. Katsamakas, E. G., & Georgantzas, N. C. (2010). Open source disruptive-innovation strategy.
15. TCMB 2010: "Finansal İstikrar Raporu", 2016 Kasım.
16. EY : Capital Markets: innovation and the FinTech landscape How collaboration with FinTech can transform investment banking.
17. KPMG (2017,Şubat): Global analysis of investment in fintech.
18. IOSCO (2017, Şubat): Research Report on Financial Technologies (Fintech).
19. Richard and Daniel Susskind (2016) : Frontiers of Financial Technology, Expeditions in future commerce, from blockchain and digital banking to prediction of markets and beyond, edited by David Shrier and Alex Pentland of MIT, 2016. Oxford University Press,
20. ECB,(2016) Occasional Paper Series: Distributed ledger technologies in securities post-trading, .

21. Ludvig Backlund (2016): A technical overview of distributed ledger technologies in the Nordic capital market, Upsala University.
22. Carlsson Jacob & Huang Shun (2016) : Blockchain Technology in the Swedish Fund Market, KTH School Of Computer Science and Communication.
23. Satoshi Nakamoto (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
24. Andreas M. Antonopoulos (2014):Mastering Bitcoin, O'Reilly Media, Inc,
25. Accenture (2015): Capital Markets, Blockchain in the Investment Bank.
26. Oliver Wyman (2016):Blockchain in Capital Markets, Euroclear.
27. UK Government Chief Scienti_c Adviser (2016). Distributed Ledger Technology:beyond block chain.
28. William Stallings (2011): Cryptography and network security : principles and practice, Boston, Prentice Hall.
29. Whit_eld Di_e and Martin E. Hellman (1976): New Directions in Cryptography.
30. Leonard Adleman Ron Rivest Adi Shamir (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.
31. Ralph C. (1988) Merkle. Advances in Cryptology | CRYPTO '87: Proceedings. Ed. by Carl Pomerance. Springer Berlin Heidelberg,. Chap. A Digital Signature Based on a Conventional Encryption Function.
32. Moni Naor Cynthia Dwork (1993), Pricing via Processing or Combatting Junk Mail.
33. Adam Back. Hashcash (2002), A Denial of Service Counter Measure.
34. Wyman Oliver (2016,Şubat): Blockchain in Capital Markets.
35. CFA İnstitute (2017): Fintech 2017: China, Asia, and Beyond.
36. ESMA (2016, Haziran) : The Distributed Ledger Technology Applied to Securities Markets, Discussion Paper.
37. Juri Mattila (2016, Mayıs): The Blockchain Phenomenon ,The Disruptive Potential of Distributed Consensus Architectures, ETLA Working Papers No:38.
38. EY : Blockchain, DLT and The Capital Markets Journey Navigating The Regulatory And Legal Landscape, Innovate Finance.
39. FCA (2017, Nisan) : Discussion Paper on distributed ledger technology, Discussion Paper.
40. Federal Reserve Board (2016): Distributed ledger technology in payments, clearing, and settlement, Working Papers in the Finance and Economics Discussion Series No: 095.
41. FINRA (2017, Ocak): Distributed Ledger Technology: Implications of Blockchain for the Securities Industry.
42. Lawrence J. Trautman : Is Disruptive Blockchain Technology the Future of Financial Services?

Yararlanılan İnternet Siteleri:

1. Bitcoinwiki. Proof-of-Stake. https://en.bitcoin.it/wiki/Proof_of_Stake.
2. Nxt. Nxt Whitepaper. http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt.
3. Scott Nadal Sunny King. Peercoin Whitepaper. https://www.peercoin.net/whitepaper.
4. https://www.cpacanada.ca/-/media/site/business-and-accounting-resources/docs/g10157-rg-technological-disruption-of-capital-markets-reporting-introduction-to-blockchain-october-2016.pdf
5. Fintech Regulation: Why the U.S. Must Look Overseas to Avoid Falling Behind, http://www.edelman.com/post/fintech-regulation-us-overseas/
6. UK regulators are the most fintech friendly, https://www.ft.com/content/ff5b0be4-7381-11e6-bf48-b372cdb1043a
7. https://www.esma.europa.eu/
8. http://www.iosco.org/
9. https://www.dunya.com/kose-yazisi/dijital-dunyanin-finans-zinciri-blockchain/372740