BAŞKENT ÜNİVERSİTESİ

SOSYAL BİLİMLERİ ENSTİTÜSÜ

TEKNOLOJİ VE BİLGİ YÖNETİMİ ANABİLİM DALI

TEKNOLOJİ VE BİLGİ YÖNETİMİ TEZLİ YÜKSEK LİSANS PROGRAMI

BLOK ZİNCİR TEKNOLOJİSİNİN BENİMSENMESİNİ ETKİLEYEN FAKTÖRLER: GÜVENLİK AÇISINDAN AMPİRİK BİR ÇALIŞMA

HAZIRLAYAN

Abdulkerim Oğuzhan ALKAN

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

Dr. Öğr. Üyesi Nurcan ALKIŞ

ANKARA-2020

BAŞKENT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 02 /12 /2020

Öğrencinin Adı, Soyadı: A. Oğuzhan Alkan

Öğrencinin Numarası: 21810466

Anabilim Dalı: Teknoloji ve Bilgi Yönetimi

Programı: Teknoloji ve Bilgi Yönetimi

Danışmanın Unvanı/Adı, Soyadı: Dr. Öğr. Üyesi Nurcan Alkış

Tez Başlığı: BLOK ZİNCİR TEKNOLOJİSİNİN BENİMSENMESİNİ ETKİLEYEN FAKTÖRLER: GÜVENLİK AÇISINDAN AMPİRİK BİR ÇALIŞMA

Yukarıda başlığı belirtilen Yüksek Lisans/Doktora tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 80 sayfalık kısmına ilişkin, 02/12/2020 tarihinde tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 16'dır. Uygulanan filtrelemeler:

1. Kaynakça hariç

2. Alıntılar hariç

3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:

ONAY

Tarih: 02 /12 / 2020

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Dr. Öğr. Üyesi Nurcan Alkış

TEŞEKKÜR

Tez çalışmam sırasında kıymetli bilgi, birikim ve tecrübeleri ile bana yol gösterici ve destek olan değerli danışman hocam Sn. Dr. Öğretim Üyesi Nurcan ALKIŞ'a, ilgisini ve önerilerini göstermekten kaçınmayan Teknoloji ve Bilgi Yönetimi Bölüm Başkanı Sn. Prof. Dr. Hakkı Okan YELOĞLU'na ve Doç. Dr. Ersin KARAMAN'a sonsuz teşekkür ve saygılarımı sunarım.

Lisans ve yüksek lisans eğitimim boyunca yardım, bilgi ve tecrübeleri ile bana sürekli destek olan Erol YÜCEL ve Teknoloji ve Bilgi Yönetimi bölümündeki tüm hocalarıma teşekkür ederim.

Çalışmalarım boyunca maddi manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme de sonsuz teşekkürler ederim.

Ankara

A.Oğuzhan ALKAN

ÖZET

A. OĞUZHAN ALKAN,

Blok Zincir Teknolojisinin Benimsenmesini Etkileyen Faktörler: Güvenlik Açısından Ampirik Bir Çalışma

Başkent Üniversitesi Sosyal Bilimler Enstitüsü, Teknoloji ve Bilgi Yönetimi Bölümü, ANKARA, 2020

Bu tez çalışmasının amacı internet bankacılığı işlemlerinde blok zincir teknolojisinin kullanımına karşı kullanıcı niyetlerini etkileyen faktörleri belirlemektir. Çalışmada nicel araştırma yöntemleri takip edilmiş ve çevrimiçi uygulan anket ile veri toplanmıştır. Araştırma evrenini; Türkiye genelinde faaliyet gösteren bankaların müşterileri oluşturmaktadır. Araştırmanın örneklemini internet bankacılığı kullanan basit tesadüfi yöntemle seçilen 356 kişiden oluşmaktadır. Toplanan veriler doğrulayıcı faktör ve Yapısal Eşitlik Modellemesi ile analiz edilerek yorumlanmıştır. Veriler dokuz faktör altında toplanmıştır: 'Davranışsal Niyet', 'Sosyal Normlar', 'Algılanan Fayda', 'Algılanan Güven', 'Algılanan Yenilikçilik', 'Algılanan Kullanım Kolaylığı', 'Bilgi Seviyesi', 'Algılanan Gizlilik' ve 'Algılanan Tatmin'.

Çalışmadan elde edilen sonuçlara göre algılanan kullanım kolaylığı ile algılanan fayda ve davranışsal niyet arasında pozitif ilişki olduğu, algılanan fayda ile davranışsal niyet arasında pozitif ilişki olduğu, yenilikçilik ve algılanan fayda arasında pozitif ilişki olduğu, gizlilik ve fayda arasında pozitif ilişki olduğu, güven ve algılanan fayda arasında pozitif ilişki olduğu, sosyal norm faktörü ile algılanan fayda ve davranışsal niyet arasında pozitif ilişki olduğu, tatmin faktörü ile davranışsal niyet arasında pozitif ilişki olduğu son olarak bilgi seviyesi ile davranışsal niyet arasında pozitif ilişki olduğu belirlenmiştir.

Anahtar Kelimeler: İnternet, İnternet Bankacılığı, Blok Zincir, Teknoloji Kabul Modeli

ABSTRACT

A. OĞUZHAN ALKAN,

Factors Affecting the Adoption of Blockchain Technology: An Empirical Study in Terms of Security

Başkent University Institute of Social Sciences, Department of Technology and Information Management, ANKARA, 2020

The purpose of this thesis is to determine the factors affecting user intentions against the use of blockchain technology in internet banking transactions. In the study, quantitative research methods were followed and data were collected with an online questionnaire. Research universe; Turkey are customers of banks operating in general. The sample of the study consists of 356 people selected by simple random method using internet banking. The collected data were analyzed and interpreted by confirmatory factor and Structural Equation Modeling. The data were collected under nine factors: 'Behavioral Intention', 'Social Norms',' Perceived Usefulness ',' Perceived Trust ',' Perceived Innovativeness ',' Perceived Ease of Use ',' Knowledge Level ',' Perceived Confidentiality 'and' Perceived Satisfaction '.

According to the results obtained from the study, there is a positive relationship between perceived ease of use and perceived usefulness and behavioral intention, a positive relationship between perceived usefulness and behavioral intention, a positive relationship between innovativeness and perceived usefulness, a positive relationship between confidentiality and utility, trust and perceived usefulness. There is a positive relationship between social norm factor and perceived usefulness and behavioral intention, and a positive relationship between satisfaction factor and behavioral intention, and finally, a positive relationship between knowledge level and behavioral intention.

Keywords: Internet, Internet Banking, Block Chain, Technology Acceptance Model

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

KISALTMALAR DİZİNİ

TKM: Teknoloji Kabul Modeli

ALFAYDA: Algılanan Fayda

AKK: Algılanan Kullanım Kolaylığı

DAVNİYET: Davranışsal Niyet

SDT: Sebepli Davranışlar Teorisi

PDT: Planlanmış Davranışlar Teorisi

ÖZYET: Özyeterlilik

AFF: Algılanan Finansal Fayda

ALYEN: Algılanan Yenilikçilik

ALTAT: Algılanan Tatmin

ALGİZ: Algılanan Gizlilik

ALGÜVEN: Algılanan Güven

SOSNORM: Sosyal Norm

BİLGİ: Bilgi Seviyesi

EĞLENCE: Algılanan Eğlence

AFA: Açıklayıcı Faktör Analizi

DFA: Doğrulayıcı Faktör Analizi

YEM: Yapısal Eşitlik Modellemesi

KEKKT: Kısmı En Küçük Kareler Testi

1. GİRİŞ

21.yüzyıl da yaşamakta olduğumuz dijital çağ büyük teknolojik gelişmeleri ve devrimleri de beraberin de getirmiştir. Bu gelişmeler karşısında sahip olduğumuz alışkanlıklarımız da değişmektedir. Gerçek anlamda internet ile başlayan bu dijitalleşme dönüşümü, veri madenciliği, mobil cihazlar, derin öğrenme, yapay zekâ, robotlar ile devam ederken, karşımıza kimi görüşlere göre internetten sonraki en büyük keşif olarak görülen blok zinciri teknolojisi gelmektedir. Özellikle karşılıklı güven mekanizmasının teknolojik olarak sağlanması, bilgilerin tek merkezi bir kaynakta toplanması yerine dağıtık yapıda olması gibi gerçekten büyük bir fikir mimarisi üzerine kurulmuş, bütün verilerin yazılım aracılığıyla birbirileriyle konuşan binlerce farklı bilgisayarda eşlenik bir şekilde tutulması gibi büyük avantajları bulunan blok zincir giderek artan bir ilgi ve kullanım alanıyla karşımıza çıkmaktadır.

1.1. Problem Durumu

Blok zinciri kavramı ilk olarak kripto para birimleri etrafında gelişim göstermiştir. Spesifik olmak gerekirse, Bitcoin gibi kripto para birimlerini takip etmek için kullanılan kayıt tutma teknolojisidir. Yabancıların çevrimiçi işlemlerinde dürüst ve tutarlı olmalarına yardımcı olan, herkesin erişebildiği merkezi olmayan bir defterdir.

Blok zincirini tam olarak anlamak için gerçek bir blok zinciri olarak hayal etmek en kolayıdır. “Bloklar” işlemler hakkında dijital bilgilerdir, “zincir” ise depolandıkları genel bir veri tabanıdır.

Bloklar, işlemin tarihi, saati ve miktarı gibi bilgiler ile bunu yapan kişinin dijital imzasından oluşmaktadır. Kişi, bir blok zinciri kullanarak aynı çevrimiçi mağazadan ikinci bir işlem oluşturacaksa, yeni blok aynı özelliklerin çoğuna sahip olacak, ancak farklı bir “karma kod” nedeniyle kataloglama kodu blok zincirleri ilkinden farklı olacaktır.

Blok zincir’e erişimi olan herhangi biri, herhangi bir zamanda görüntülemek için bir kopyasını çıkarabilir; bu, herhangi bir noktada, bir blok zincirinin binlerce kopyasının çalıştığı anlamına gelmektedir. Bir bilgisayar korsanının blok zincirini manipüle etmesi için, eşzamanlı olarak mevcut tüm kopyalarını manipüle etmeleri gerekir ve bu çevrimiçi bilgisayar korsanlarının ve dolandırıcılık sanatçılarının yapabileceklerinin çok ötesinde bir görevdir.

Ayrıca bilgiler bu dijital imza sayesinde güvende tutulur. Verilen miktar ve tarih gibi işlemin bağlamsal detayları dışında bloğa herhangi bir bilgi vermenize gerek yoktur ve sizinle ilgili tek bilgi dijital imzadır.

İşlemlerle ilgili bu tam bir coğrafi bağlam eksikliği ile (IP adresleri bile blok zincirlerinde saklanmadığından), işlemler, dışarıdan birine neredeyse anlamsız veri listelerine indirgenir. Kayıtlar zincir sayesinde vardır, fakat bu kimsenin işine yaramamaktadır.

Bitcoin'in blok zinciri, Haziran 2019 itibarıyla 580.000 bloğun üzerindedir ve bu sadece her geçen dakika artmaktadır. Bu blok zincirini düzenlemek için gereken hesaplama gücü basitçe mevcut değildir. Blok yapıldıktan sonra düzenlenemez ve sakladığı veriler güvendedir.

Çevrimiçi bankalar, iş yapma şekillerini büyük ölçüde değiştirme şansı olduğu için blok zincir teknolojisiyle ilgilenmektedir. İşlemler şu anda bankanın fiili çalışma saatleriyle sınırlıdır. Blok zinciri haftanın 7 günü, günde 24 saat çalışır ve bu bankaların karşılaştığı işlem sürelerini önemli ölçüde hızlandırabilir. Bankalar zaten bunun nasıl uygulanabileceğini araştırmaktadır ve belki de bunun yaygın bir uygulama haline gelmesi çok uzun sürmeyecektir.

Finans sektöründen beklenenin çok ötesine yayılan güvenli veri depolama uygulamaları ile blok zincir teknolojisinin güvenli kayıtlar ve özel işlemlerde bir sonraki adımımız olduğu açıktır. Hem bankacılık sektörüne hem de günlük hayatımıza getirebileceği değişiklikler harika olacaktır.

Blok zincirine geçiş, geleneksel bankacılık uygulamalarının geçmişiyle karşılaştırıldığında hala ilk aşamalardadır. Fikir prensipte güzel, ancak kolaylık faktörü hala orada değildir. Birçok kişi nakit parayı tercih eder ve bu nedenle kanıtlanmış uygulamalara dayalı geleneksel bir fiziksel bankayı tercih etmektedir.

Cocco vd. (2017), blok zinciri teknolojisinin bankacılıkta uygulanmasının zorluklarına ve fırsatlarına bakmaktadır ve bu yıkıcı teknolojinin potansiyelleri hakkında düşünmek için yiyecek sağlamaktadır. Blok zincir teknolojisi, şu anda olduğundan daha verimli sistemler kullanarak, küresel finansal altyapıyı optimize edebilir, sürdürülebilir kalkınma sağlayabilir. Aslında, birçok banka şu anda ekonomik büyümeyi teşvik etmek ve yeşil teknolojilerin gelişimini hızlandırmak için blok zincir teknolojisine

odaklanmaktadır. Blok zincir teknolojisinin finansal sistemi destekleme potansiyelini anlamak için, Bitcoin sisteminin gerçek performansı incelenmiş ve aynı zamanda gereken yüksek hesaplama gücü nedeniyle önemli enerji tüketimi ve yüksek maliyet gibi temel sınırlamaları vurgulanmıştır.

Hassani vd., (2018) Blok zincir'in bankacılık sektörünü bozmakta ve bankacılıkta artan büyük veriye katkıda bulunmakta olduğunu belirtmişlerdir. Bununla birlikte, akademik açıdan bankacılıkta blok zincir tabanlı büyük veriye yönelik araştırma ve geliştirmede bir boşluk var ve bu boşluğun, bankacılık için blok zincir teknolojisinin benimsenmesi ve geliştirilmesi üzerinde önemli bir olumsuz etkisi olması beklenmektedir. Akademisyenler, araştırmacılar ve bankacılar tarafından daha aktif katılımı motive etmek umuduyla, bankacıların bakış açısıyla fırsatları ve zorlukları özetleyerek blok zincirinin bankacılıktaki etkisinin bugüne kadarki en kapsamlı incelemeyi yapmışlardır. Ek olarak, blok zincirinden elde edilen büyük verilerin gelecekte bankacılık veri analitiği üzerindeki etkisini de tartışmakta ve bankacılık endüstrisi için filtreleme ve sinyal çıkarmanın artan önemini belirtmektelerdir.

Guo ve Liang (2016) yapmış oldukları çalışma ile blok zincir teknolojisinin bankacılık endüstrisinde gelecek vaat eden uygulama beklentilerine sahip temel bir teknoloji olduğunu belirtmişlerdir. Bir yandan, Çin'deki bankacılık sektörü, daralan faiz oranı farkının neden olduğu faiz oranlarının serbestleştirilmesi ve kâr düşüşünün etkisiyle karşı karşıyadır. Öte yandan ekonomik dönüşüm, internet gelişimi ve finansal yeniliklerden de etkilenmektedir. Bu nedenle, bankacılık sektörü acil dönüşüme ihtiyaç duymakta ve yeni büyüme yolları aramaktadır. Böylelikle, blok zincirleri, bankalardaki ödeme takas ve kredi bilgi sistemlerinin altında yatan teknolojide devrim yaratabilir, böylece onları yükseltir ve dönüştürür. Blok zinciri uygulamaları aynı zamanda bankacılık sektörünün verimliliğini artıracak "çok merkezli, zayıf aracılıklı" senaryoların oluşumunu da teşvik etmektedir. Ancak, Blok zincirlerin izinsiz ve kendi kendini yöneten doğasına rağmen, merkezi olmayan bir sistemin düzenlenmesi ve fiilen uygulanması çözülmesi gereken sorunlardır.

Blok zincir hakkındaki akademik çalışmaların yaklaşık %80'i Bitcoin odaklıdır. Araştırmaların %20'den daha az kısmıysa akıllı kontratlar dahil olmak üzere blok zincir uygulamaları üzerinde durmuşlardır. Buna ilaveten, verimlilik kapasitesi ve gecikme süresi gibi blok zincirin ölçeklenebilirlik hakkındaki sorunlarını araştırmacılar dikkate almamıştır.

Blok zincirin, büyük ölçekte ve bilhassa bankacılıkta ele alınabilmesi için, kendisini tam anlamıyla ispatlamamış olmasına karşın gerek akademi gerekse de özel Ar-Ge merkezleri ölçeklenebilirliği ve sunabileceği çözümler bakımından yoğun araştırmalar gerçekleştirmektedir. Bu araştırmalar, ileri kriptografik, dağıtık sistemleri ve oyun kuramını araç olarak ele almaktadır.

Blok zincir gibi yeni teknolojilerin yayılımı ve etkin kullanımı son kullanıcıların bu teknolojilere karşı tutumlarına bağlıdır. Literatür taramasında blok zincir teknolojisinin internet bankacılığı işlemlerinde kullanılmasına karşı kullanıcıların tutumlarını araştıran spesifik çalışmalara denk gelinmemiştir. Bu tarz yeni teknolojilerin yayılımında kullanıcı tutumları önemli olduğu için bu tez çalışması kapsamında kullanıcıların internet bankacılığı işlemlerinde blok zincir kullanımına karşı niyetleri araştırılmıştır.

1.2. Araştırmanın Kapsamı

Bu tez çalışmasında bilişim sistemleri araştırmalarında kullanıcıların yeni teknolojilere karşı tutumlarını açıklamada en yaygın kullanılan modellerden biri olan Teknoloji Kabul Modeli temel alınarak blok zincir teknolojisinin internet bankacılığı işlemlerinde kullanımına karşı kullanıcıların tutumlarını açıklayan bir yapısal model sunulmuştur. Sunulan araştırma modelinde gizlilik, güven, tatmin, algılanan fayda, algılanan finansal fayda, eğlence, davranışsal niyet, yenilikçilik, öz yeterlilik, algılanan kullanım kolaylığı, sosyal norm ve bilgi seviyesi faktörlerinin etkileri araştırılmıştır.

1.3. Çalışmanın Amacı

Bu çalışmanın üç tane amacı vardır: (1) Blok zincir teknolojisinin internet bankacılığı işlemlerinde kabulünü etkiyen faktörleri belirlemek, (2) İnternet bankacılığı işlemlerinde blok zincir kullanımına karşı kullanıcı benimsemelerini açıklayana bir teknoloji kabul modeli sunmak, (3) literatüre ve blok zincir kullanımına katkı sağlamak.

1.4. Araştırma Soruları

Aşağıdaki 2 araştırma sorusu etrafında bu çalışma şekillendirilmiştir:

1-) Kullanıcıların internet bankacılığı işlemlerinde blok zincir teknolojisini kullanma niyetlerini etkileyen faktörler nelerdir?

2-) Güvenlik ve gizlilik faktörleri, internet bankacılığı işlemlerinde blok zincir kullanımını nasıl etkilemektedir?

1.5. Çalışmanın Önemi

Blok zinciri teknolojisi, internetin icadından sonra gelen yıkıcı ve devrim niteliğindeki yeniliklerden biri olarak kabul edilmektedir. Blok zincir teknolojisi günden güne iş dünyasında önemli bir yer edinmeye devam etmektedir. Birçok blok zinciri uygulaması, dijital verileri kriptografi kullanımı yoluyla kaydeden ve koruyan dağıtılmış bir defter olarak işlev görmektedir. Yapılan bu araştırma da blok zincir tabanlı internet bankacılığı sistemlerinin kullanıcılar tarafından benimsenmesi araştırılmış ve yapısal bir model doğrulanmıştır. Doğrulanan modelde kullanıcıların internet bankacılığı işlemlerinde blok zincir teknolojisini benimsemesini etkileyen faktörler algılanan kullanım kolaylığı, algılanan fayda, yenilikçilik, gizlilik, güven, tatmin, sosyal norm ve bilgi seviyesi olarak belirlenmiştir. Yapılan literatür taramasında blok zincir teknolojisinin internet bankacılığı işlemlerinde benimsenmesini açıklayan bu kadar kapsamlı bir modele rastlanmamıştır. Bu nedenle bu tez çalışması bu alandaki literatüre katkı sağlamayı hedeflemiştir.

1.6. Tez Çalışmasının Aşamaları

Bu tez toplam 9 bölümden oluşmaktadır. Tez çalışmasına literaratür taraması ile başlanmıştır. Literatür taraması giriş bölümünden sonra 3 bölüm halinde sunulmuştur. 2. bölümde blok zincir teknolojisini, tanımını, yapısını, kullanım alanlarını, bugüne kadar bu alanda yapılan çalışmalar sunulmuştur. 3. Bölümde blok zincir teknolojisinin internet bankacılığında nasıl kullanıldığını ve ne amaçlı kullanıldığını güvenlik bakış açısıyla anlatılmıştır. 4. Bölümde çalışmanın kuramsal çerçevesini oluşturan teknoloji kabul modeli sunulmuştur.

5. Bölümde araştırma modeli sunulmuş ve araştırma değişkenleri tanımlanarak ilgili hipotezler verilmiştir. 6. bölümde çalışmanın örneklem bilgisi, veri toplama aracı ve veri analizine yönelik bilgiler verilmiştir. 7. bölümde veri analizi ve bulgular detaylı bir şekilde verilmiştir. Son olarak elde edilen bulgular tartışılmış ve tez çalışması sonlandırılmıştır.

2. BLOK ZİNCİR TEKNOLOJİSİ

2.1. Blok Zinciri Tanımı

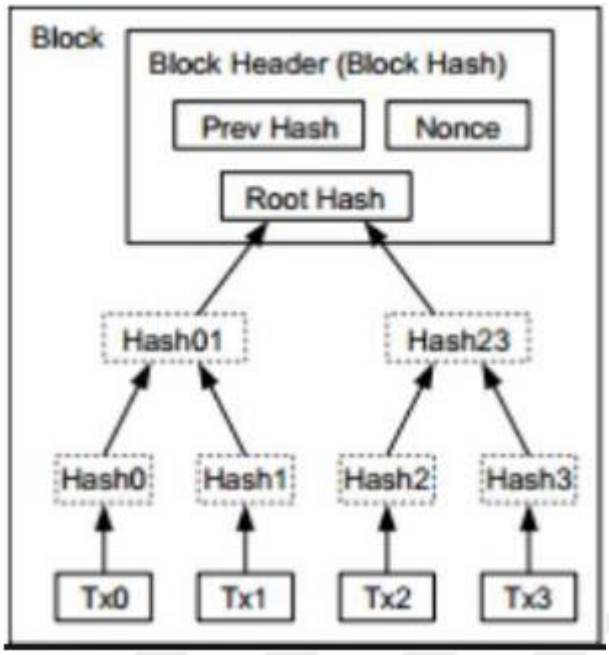
Blok zinciri teknolojisi, internetin icadından sonra gelen yıkıcı ve devrim niteliğindeki yeniliklerden biri olarak kabul edilmektedir. Blok zincir teknolojisi günden güne iş dünyasında önemli bir yer edinmeye devam etmektedir. Birçok blok zinciri uygulaması, dijital verileri kriptografi kullanımı yoluyla kaydeden ve koruyan dağıtılmış bir defter olarak işlev görür. Bu nedenle dağıtık hesap defteri (distributed ledger) olarak nitelendirilebilecek olan blok zinciri; temelde birden fazla tarafın kendi aralarında önden mutabakata vararak hataları sıfıra indirip, işlemi farklı veri tabanları üzerinde kaydederek değiştirilememesini garanti altına aldıkları bir veri saklama yaklaşımı özelliğini taşır. Bir değer taşıyan her işlem, matematik ve kriptoloji aracılığıyla dağıtık ve bir otoritenin yönetmediği bağımsız veri zincirleridir. Kriptografi kullanımı ile kullanıcılarına çoğunlukla bir merkez olmaksızın, aynı anda birden fazla noktadan kontrol edilebilen ve olguların durumu hakkında güvenilir fikir birlikleri sağlamayı garanti eden blok zinciri teknolojisi sayesinde; veri, yetkilendirmeler ölçüsünde paydaşlar ile paylaşılmakta olup işlemlerin tutarlılığı ve doğruluğu sağlanmaktadır. Diğer bir deyişle; bir işlemin gerçekleşmesi ekosistem içerisinde yetkisi olan paydaşların onayına tabi olup, işlem bilgisi merkezi olmayan bir yapıda tüm paydaşlarda kayıt altına alınmakta ve sistem içerisinde gerçekleştirilen her işlem bir önceki işleme bağlı tutulmaktadır (Durbilmez, 2018).

2.2. Blok Zinciri Yapısı

Bir blok zinciri sistemi, çalışma mekanizması ve mutabakata varmak için hangi yöntemlerin kullanılacağı konusunda düzenlenebilmektedir. Bu sistem küçük gruplar arasında ya da çok fazla üyesi olan yapılarda da kullanılabilmektedir. Bu yapıya en güzel örneklerden biri olarak milyonlarca üyesi olan Bitcoin verilebilir.

2.2.1. Blok

Blok zincirini, onaylanmış ve güvenli bir şekilde birbirine bağlanmış bilgi blokları oluşturmaktadır. Blok zincirindeki her bir blok, başlık ve gövde olarak 2 ana bölümden oluşmaktadır. Blok başlığı içerisinde; Blok Versiyon Numarası, Önceki Blok Özet Değeri, Zaman Damgası, Zorluk Derecesi, Nonce ve Merkle Kök Özeti bulunmaktadır. Blok gövdesinde; Blok Özet Değeri ve Blok işlemleri yer almaktadır.



Şekil 1 Blok Başlığı ve Gövdesi

2.2.2. İşlem/Hesap Hareketi

Bilgi bloklarının içerisinde tutulan veriler, hesap defter girişini ya da hesap hareket kayıtlarını (işlemleri) temsil etmektedir. Her hesap hareketinin dijital olarak imzalanarak gerçekliğinin korunması sağlanmaktadır. Böylece kayıt üzerinde kimse değişiklik yapamaz ve verinin güvenilir olduğu varsayılır. Blok zincir ağında terminaller arasındaki varlık transferlerinin kayıtlarına işlem denir. Bu işlemler blokların gövdesinde saklanır. Temel olarak bir işlem; Toplam Miktar, Girdi Listesi, Çıktı Listesi, Özet Değeri bilgilerinden meydana gelir;

- Toplam miktar, transfer edilecek dijital varlıkların toplam miktarı bilgisini tutar,
- Girdi listesi bilgi olarak transfer edilecek varlıkların listesini, miktarlarını ve gönderici hesap adresini tutar,
- Çıktı listesi bilgi olarak transfer edilecek varlıkların miktarlarını, alıcı adresini ve yeni sahiplerini tutar,
- Özet Değer, işlem içeriğinin hesaplanmış kriptografik özet değeridir. Özet değer kullanılarak, saklı anahtar ile işlemler imzalanır ve göndericinin açık anahtarı kullanılarak doğrulanır.

2.2.3. Hesap Adresleri

Blok zincirinde yer alan bir işlemde, gönderici ve alıcının hesap adresleri yer almaktadır. Sisteme dâhil olan her yeni kullanıcı için yeni bir adres üretilir. Bu adresler

blok zincir sisteminde kullanıcıların kimlikleri niteliğindedir. Kullanıcının açık anahtarları kullanılarak hesap adresleri oluşturulur. Bu adreslerde, dijital bir varlığın sahiplik bilgisi tutulur. Bir kullanıcının sahip olduğu dijital varlığı kullanarak işlem yapabilmesi için, o hesaba ait saklı anahtarının olması gerekir. Çünkü işlemlerin, kullanıcının saklı anahtarı ile imzalanmış olması gerekmektedir. Yaratılan bu işlemin doğrulanmasında hesap adresinden oluşturulan açık anahtar kullanılmaktadır.

2.2.4. Kayıt Defteri/Hesap Defteri

Veriler, her terminalde yer alan herkese açık hesap defterlerinde tutulmaktadır. Bu hesap defterleri içerisinde blok zincir ağında oluşturulan ve doğrulanan işlemler yer almaktadır. Sistem güvenliği, dijital hesap defterlerinin bir altyapı ya da ağ üzerinde dağıtılmasıyla sağlanmaktadır. Altyapıdaki bu ek katmanlar, bir hesap hareketinin durumu ile ilgili istenilen her an mutabakat sağlanabilmesi amacına hizmet etmektedir. Her katmanda, gerçekliği korunan hesap defterlerinin kopyası yer almaktadır. Sisteme yeni bir hesap hareketi geldiğinde ya da mevcut bir işlemde değişiklik yapıldığında, altyapıda yer alan tüm kayıtlarda belirli bir algoritma çalışarak bu yeni işlemin doğruluğunu kontrol etmektedir. Hesap defterleri kopyalarının çoğunluğu bu kaydın doğruluğunu onaylarsa, yeni bir blok sisteme dahil edilmektedir. Eğer sistemdeki kopyaların çoğunluğu yeni işlemi reddederse, bu hesap hareketi sistem üzerine kaydedilemeyecektir. Bu dağıtık sistem sayesinde, Blok zinciri merkezi bir yapı ile kontrol edilmeden etkili bir şekilde çalışmaktadır (Durbilmez, 2018).

2.2.5. Cüzdan

Kişilerin saklı anahtarları çok önemlidir. Dijital varlıkların güvenliği için bu anahtarın çok sağlam ve güvenli bir şekilde saklanması gerekmektedir. Cüzdan, bu anahtarların saklandığı uygulamalardır. Cüzdanlar, ek olarak kullanıcıya ait dijital varlık bilgilerini ve açık anahtarı da gösterir. Uygulama, yerel diskler üzerinde ya da bulut içerisinde yer alır.

2.2.6. Kriptografik Hash Fonsiyonu

Kriptografi, kısaca bir verinin şifrelenmesi anlamına gelmektedir. Bu şifreleme işlemi, karmaşık olan birçok gelişmiş matematiksel tekniği kullanan derin bir akademik araştırma alanını kapsamaktadır. Burada bilinmesi gereken ilk şifreleme tekniği temel bir şifreleme olan hash işlevidir. Hash birçok kaynak ve uygulamada İngilizce olarak kullanılsa da Türkçe karşılığı itibariyle bilişim dünyasında özetleme olarak ifade

edilmektedir. MD-5, SHA-1, SHA-2, SHA-3, BLAKE gibi farklı özetleme algoritmaları bulunmaktadır. Bir hash, üç temel özelliğe sahip matematiksel yöntemdir. Bunlar (Karaköse, 2017);

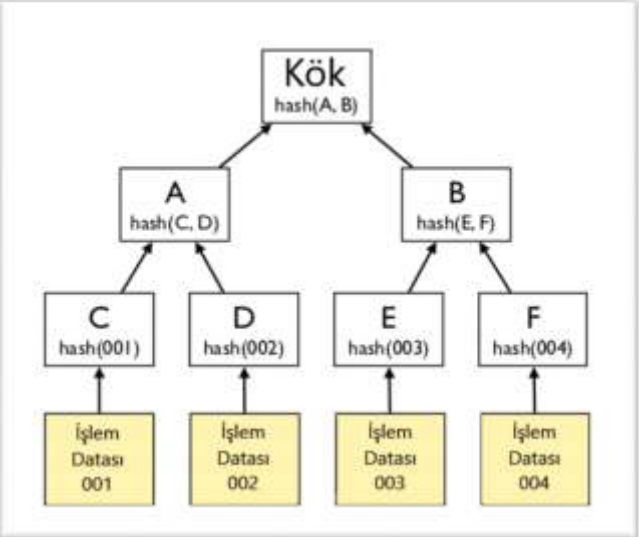
- Girdi verileri herhangi bir boyutta herhangi bir dize olabilir,
- Sabit boyutta bir çıktı üretmektedir. Örneğin; 64, 128, 256 bit çıktı boyutu,
- Verimli olarak hesaplanabilmektedir. Sezgisel olarak, belirli bir girdi dizgesi için, hash çıktısının makul bir süre içerisinde ne olduğunu bulabileceğiniz anlamına gelmektedir.

Bir kriptografik işlem özet fonksiyonun da H:{0,1} $*$ $\rightarrow$ {0,1}n herhangi bir istenilen uzunluktaki mesaj olan M için n bitlik bir sabit uzunlukta hash değerini hesaplayan bir fonksiyondur. Kriptografik hash fonksiyonu, dijital imza şemaları, kimlik doğrulama kodları, parola işlem özet fonksiyonları ve içerik adresli depolama da dahil olmak üzere pek çok uygulamada kullanılan temel bir kriptografi yöntemidir. Bu uygulamaların birçoğunun güvenliği veya düzgün işleyişi, kırılmasının (çarpışmaların bulunmasının) pratik olarak mümkün olmadığı varsayımına dayanmaktadır. Güvenli Hash Algoritması (SHA-Secure Hash Algorithm), bir dizi kriptografik hash işlevinden oluşmaktadır. Özetle kriptografik hash, bir metin veya veri dosyası için bir imza gibidir. SHA-2 Hash Algoritmasının, 6 farklı fonksiyonundan biri olan ve yüksek güvenliğe sahip olanı SHA-256 algoritmasıdır. Bu algoritmada farklı boyut ve büyüklükteki yazı, sayı veya değişik formattaki bilgisayar dosyası verileri, tek yönlü olmak üzere standart büyüklükte, 256 bit (32 byte-64 hexadecimal) boyutunda özetleme değerlerine dönüştürülmektedir. Aynı veri için hesaplanan SHA-256 değeri her zaman aynı sonucu vermektedir ve sadece veri de değişikliği olması durumunda sonuç özetleme değeri değişmektedir.

2.2.7. Merkle Tree (Ağacı)

İngilizce ifadesiyle Merkle Tree, Merkle Root veya Root Hash, Türkçe ifadesiyle ise Merkle Ağacı, Merkle Kökü veya Kök Özet tanımları aynı anlamda kullanılmaktadır. Genel anlamda, Merkle Ağacı büyük veri yığınlarının bir araya getirilip özet olarak gösterilmesi ve bunun güvenli bir şekilde doğruluğunun sağlanabilmesidir. Çalışma prensibi açısından bir ağacın yapısına benzemektedir. Ağacın yaprakları veri bloklarını temsil etmekte, bu veri blokları özetleme fonksiyonundan geçirilerek özet değerleri oluşmakta ve bunlar da ağacın dallarını temsil etmektedir. Oluşan özet değerlerde tekrar özetleme fonksiyonlarından geçirilerek yeni özet değerler elde edilir. Bu döngü aynı

şekilde devam ederek en son kök özet değerine ulaşılır. Bu da ağacın köküne ulaşmak olarak yorumlanmaktadır. Anlatılan bu yapı aşağıdaki şekilde gösterilmiştir (Karaköse, 2017).



Şekil 2 Örnek Merkle Ağacı Yapısı

2.3. Blok Zincir Çeşitleri

2.3.1. Genel Blok Zincirleri

Bir genel blok zincirini, dünyadaki herhangi bir kişi okuyabilmekte, işlem yapabilmekte, yapılan işlemin geçerli olması durumunda sonuçlarını görebilmekte ve uzlaşma sürecine (mevcut durumun ne olduğu ve hangi blokların zincire ekleneceğinin belirlenmesi sürecine) katılabilmektedir. Kimseye erişim kısıtlaması yapılmamaktadır. En gelişmiş ve en çok bilinen genel blok zincirlerine örnek olarak Bitcoin ve Ethereum verilebilir.

2.3.2. Özel Blok Zincirleri

Özel blok zincirinde ağa katılacak ve onay işlemi yapacak kişilere izin verilmesi gereklidir. Ağ yöneticileri tarafından davet edilmedikçe katılım sağlanamayacaktır. Hassas verileri, herkese açık olan bir yapıda riskle karşı karşıya bırakmamaktadırlar. Herhangi bir muhasebe mevzuat sistemine ve resmi kayıt işleme prosedürlerine bağlı olmadan kendi içerisinde kayıt tutmaya çalışmaktadırlar (Durbilmez, 2018).

2.3.3. Konsorsiyum Blok Zincirleri

Bir konsorsiyum blok zincirinde ağa katılacak kişilere izin verilmesi gereklidir. Fakat bunu, özel blok zincirindeki gibi tek bir kuruluş kontrol etmez. Ortak yapıya dahil olan her şirket, ağ üzerinde bir düğüm işletebilmektedir. Konsorsiyum blok zincirinde,

zincirin yöneticileri tarafından kullanıcıların okuma hakları kısıtlanmaktadır ve az sayıda güvenilir düğümlerin bir konsorsiyum protokolü işletmesine izin vermektedir.

2.4. Blok Zinciri Alt Yapısı

Hyperledger, Linux tarafından fonlanan, iş uygulamalarını hedefleyen ve IBM'in ev sahibi olduğu Blok Zinciri tabanlı modüler yaklaşım bir Blok Zinciri çatı platformudur. Genellik ve esneklik kavramları üzerine inşa edilmiş olup temel tasarım olarak geniş bir yelpazede akıllı sözleşmelere destek verir. Bu sistemin temel bir özelliği de, genişleyebilir oluşu ve özellikle Blok Zinciri oluşturmak için çoklu hizmet alt yapı araçları sağlayabiliyor olmasıdır. Blok Zinciri yönetimi için birden fazla akıllı sözleşme kullanım olanağı sağlar (Sousa, 2018).

Tipik olarak eşler arası, bir ağ içinde konuşlandırılmış ve dağıtılmış bir verinin kaydını tutan açık bir veri tabanıdır. Blok Zincirin temel mantığıyla eş misyon, işlemleri (Transaction) içeren, blok ve sürekli büyüyen bir kayıt listesinden oluşur. Bloklar, kriptografik karmalar (hash) ve uzlaşma mekanizması tarafından müdahalelere karşı korunmaktadır. Blok Zinciri, izin verilen ya da izne gerek olmaksızın modele bağlı kalabilir. İzne gerek olmaksızın kayıtlar, merkezi olmayan ve anonim bir şekilde DLT (Distributed Ledger Technology) tarafından muhafaza edilebilir (Cachin, 2016).

2.4.1. Blok Zinciri Alt Yapısı Çatısı

Hyperledger, içerisinde bir açık kaynak projesinin çatısını oluşturmaktadır. Çeşitli bileşenlerin eklenebildiği uygulamalar ve bunlar için var olan akıllı sözleşmeleri desteklemek amacıyla izne gerek olmayan bir Blok Zinciri sistemidir. Fabric kullanıcıları, "Chaincode" kullanarak işlemlerini yönetmek için, akıllı sözleşmeleri kullanırlar. Chaincode'lar; Fabric içerisinde akıllı sözleşmelerin tam eşleniğidir. Fabric üzerinde işlenmiş olan kodlar, veri tabanınında (sürümlü bir anahtar olarak modellenmiştir) ve onay ilkelerine uygun davranan, onaylayan eşlenikler tarafından yürütülür ve tamamlanır. Servis, sorumlu olduğu işlemi eklemek için blok dağıtımın yanı sıra her komut ile de Kayıt Defterine (ledger) eklenir. Servis sağlayıcısının sorumluluğu, her eklenen blok için dağıtık kayıt defteri atamak, hem de hangi blokların deftere ekleneceğine karar vermektir (Sousa, 2018).

2.4.1.1. Hyperledger Fabric Protokolü

Onaylanan eşler tarafından yürütülüp geçerli kılınan ve veri tabanının durumunu onay ilkelerine bağlı olan bir koddan oluşur. Fabric Protokolü, dağıtık defter için bloklar oluşturmaktan ve her bloğun deftere eklendiği hizmetlerden sorumludur.

- Adım 1: İstemciler bir eş misyon faaliyeti yaratıp eşlenikler için mesaj gönderirler. Bu mesaj bir zincir kodu fonksiyonunu işleme çağırmak için kullanılır. Bu durum bir zincir kodunu ID (Kimlik)'e dahil etmek amacıyla ve zaman süresi ile işlem yükünü belirlemek amacıyla yapılır.
- Adım 2: Onaylanan eşlenikler eş misyon eylemlerini benzetirler ve bir uzlaşma anlaşması imzalarlar. İstemci uygun biçimde yetkili kılındıysa, bir zincirin erişim kontrol politikalarını değerlendirerek işlemi gerçekleştirebilir. İşlemler daha sonra mevcut duruma göre yürütülür. Eşlenikler istemciye bu oluşumun sonucunu iletir (mevcut durumlarıyla ilişkili "node"ları okuyabilir ve yazabilir). Bu noktada ek bir güncelleme yapılmaz.
- Adım 3: İstemciler eş misyon fonksiyonunu toplayabilirler ve birleştirebilirler. İstemciler karara varmak amacıyla eşlenikleri onaylar, eğer kümelerin okuma ve yazma sonuçları eşleniklerle uyuşursa onay politikası yerine getirilmiş demektir. Eğer bu şartlar sağlanırsa, istemciler onaylı bir okuma yazma kümesini barındıran "zarf" yaratır, bu zarfın içinde onaylı kanal ID'si de bulunur. Kanal, Fabric ağı içerisinde özel bir Blok Zinciri ve veri bölümünü sağlayan noktadır. Kanalın her bir eşleniği, kanalın spesifik kayıt defterini paylaşır. Bahsi geçen söz konusu zarf, bir işlemi temsil eder.
- Adım 4: İşlemciler eş misyon eylemi yayını için öneri sunarlar. Hizmet sağlayıcı, zarfın içeriği okumaz. Yalnızca ağdaki tüm kanallardan zarf toplar, zarfları yönlendirir ve bu zarfları içeren işaretli blok zincirlerini oluşturur.
- Adım 5: Zarf; blokları kanaldaki eşleniklere iletir. Blok içindeki zarflar onay politikalarını sağlamak ve yerine getirmek amacıyla okuma seti değişkenleri için eş durumlarında değişiklik olup olmadığını kontrol etmek için (okuma seti işlem yürütücüsü tarafından üretildikten itibaren) kontrol edilip doğrulanır. Bu maksatla, okuma seti bir işlemi benzetimler iken, eşleniklerin okunmasını sağlayan bir dizi sürümlü anahtar içerir. Bu doğrulamaların başarısına bağlı olarak, zarflar içerisinde bulunan hareket önerisi geçerli veya geçersiz olarak işaretlenir.

- Adım 6: Eşler, alınan bloğu kanalın blok zincirine bağlar. Her geçerli işlem için, yazma kümeleri eşlerin mevcut durumları için kararlılık gösterir. İstemciye, işlemin kanalın blok zincirine kesin olarak eklendiğini bildirmesi için bir olay tetiklenir, işlemin geçerli veya geçersiz kabul edilmesine karar verilir. Geçersiz işlemlerin de deftere eklendiğine dikkat edilir, ama eşleniklerde bu durum geçerli olmaz. Bu aynı zamanda, kötü niyetli istemcileri tespit etmeyi mümkün kılma avantajını da beraberinde getirir, çünkü eylemleri de kaydedilir (Sousa, 2018).

Fabric protokolünün önemli yönü, onaylamanın (2.adım) ve onaylamanın (5.adım) farklı eşleniklerde yapılabilmesidir. Ayrıca, onay sırasında zincir kod uygulamasının aksine, onaylama kodunun deterministik olması gerekmektedir. Yani aynı durumdaki farklı eşler tarafından onaylanan aynı işlem aynı çıktıyı üretecektir.

2.4.1.2. Düzenleme ve İyileştirme

Hizmet servisinin uygulanması, bütünlüğünü korumayı amaçlayan blok başına tek bir imza ile sağlanır. Fabric her bloğun kendisiyle ilişkilendirilmiş iki imza içermesini bekler. Biri imzanın ilişkili bloğun bütünlüğünü koruması amaçlanırken, diğeri blok işlemlerini bir yürütme bağlamında adapte edebilmek için tasarlanmıştır. Bununla birlikte, sınırlayıcı faktör imza oluşturma oranı, yani veri boyutu küçük ön sınırı olan küçük işlemler olduğunda, bu önemli bir performans düşüşüne yol açabilir. Temel olarak normal yükü ve son yapılandırma zarfını depolayan bir bloğun kimliğini kapsadığı için; ikinci imzayı almak için yeterli neden bulunmamaktadır. Sadece ilk imzanın üretilmesinin Blok Zincirinin bütünlüğünü korumak için yeterli olduğu anlaşılmaktadır. İstem düğümlerinden kötü niyetli davranışlara karşı her biri yerel olan bloklar toplanır ve imzalarını üretirler. Bu da, defterin ön uçlarında tutulan yerel kopyalara eklenen bir blok akışı ile sonuçlanır.

Ancak Fabric kod temeli, bir blok akışı yerine zarf akışını üreten ve yalnızca kilitlenme emri veren servisler için daha uygundur. Örneğin, bir zarf akışı aldıktan sonra fabric, hem blok oluşturmak hem de bunları zincire eklemek için yöntemler kullanır. Ayrıca, blokları zincire ekleyen yöntemler de daha önce tartışılan imzaları oluşturur. Blok Zinciri, üzerinden bağlı düğümler tarafından işletilen, dağıtılmış bir protokol aracılığıyla "Güvenilir" bir bilgisayar servisine benzer. Hizmet, tüm düğümlerin bir miktar hissesine sahip olduğu bir varlığı temsil eder veya yaratır. Düğümler hizmeti yürütme hedefini paylaşır, ancak daha fazlası için mutlak biçimde birbirlerine güvenmezler. "İzinsiz" bir Blok Zincirinde, herkes bir düğümü çalıştırabilir ve CPU döngülerini harcama yoluyla

işleme katılabilir ve bir "iş güvenliği" örneği sergileyebilir. Öte yandan, onaylama ve protokolde yer alan "izinli" model kontrolündeki bloklar, bu düğümler ile tipik olarak kimlikleri oluşturabilir ve bir uzlaşma protokolü ortaya koyabilirler. Hyperledger Fabric, akıllı sözleşmeler yapmak için dağıtık bir defter platformu kullanan, çeşitli fonksiyonların takılabilir uygulamalarına izin veren modüler bir yapıya sahip olan, bilinen ve kanıtlanmış bir teknolojidir (Cachin, 2016).

2.4.2. Çatı Mimarisi

Fabric Blok Zinciri, bir ağı oluşturan bir dizi düğümden oluşur. Yapıya izin verildiği için, ağa katılan tüm düğümlerin modüler bir üyelik servis sağlayıcısı (MSP) tarafından sağlanan bir kimliği vardır. Bir Fabric ağındaki düğümler aşağıdaki üç rolden birini üstlenirler:

- İstemciler, işlem tekliflerinin yürütmek için bilgi sunumu yaparlar, yürütme aşamasını düzenlemeye yardım eder ve son olarak sipariş vermek için işlemleri yayınlarlar.
- Eşler, işlem tekliflerinin yürütür ve işlemleri doğrularlar. Tüm eşler, bir karma zincir şeklinde, tüm işlemler deftere kaydedilene dek, ekleme yaparak veri yapısını korurlar. Tüm eşler tüm işlemleri yürütmezler. Teklifler, yalnızca onaylayan eşler (veya basitçe onaylayıcılar) olarak adlandırılan alt küme tarafından, işlemin ilgili olduğu zincir kod politikasında belirtildiği şekilde yürütülür. Geçerlilik aşamasında değerlendirilen bir onay politikası, güvenilmeyen uygulama ve geliştiricileri tarafından seçilemez veya değiştirilemez. Bir onay politikası, yalnızca zincir kodu ile parametrelendirilebilen, Fabricteki işlem doğrulaması için statik bir kütüphane görevi görür. Yalnızca belirlenmiş yöneticiler, onay politikalarını sistem yönetimi fonksiyonları ile değiştirme iznine sahip olabilir. Tipik bir onay ilkesi, zincir kodunun, bir işlem için onaylayanları, onay için gerekli olan bir grup eşlenikler biçiminde belirtmesini sağlar. Setlerde "beşte üç" gibi matematiksel monoton bir ifade kullanılır.
- Hizmet Servis Düğümleri (OSN) veya sadece hizmet verenler, hizmet servisinin toplu olarak oluşturan düğümlerdir. Kısacası, sipariş hizmeti, her işlemin yürütme aşamasında hesaplanan durum güncellemelerini ve bağımlılıkları içerdiği için tüm işlemlerin toplam sırasını belirler. Onaylayan eşler, kriptografik imzaları ile birlikte onaylayarak bir eş şifreleme imzası oluşturur. Bu tasarım seçimi, Fabric'te fikir

birliğini mümkün olduğunca modüler kılar ve fikir birliği protokollerinin değiştirilmesini basitleştirir.

Bir istemci, onay ilkesi gereği belirtilen protokoller vasıtasıyla işlem talebi gönderir. Her işlem daha sonra belirli eşler tarafından gerçekleştirilir ve çıktısı kaydedilir. Yürütmeden sonra, işlemler, bloklar halinde gruplandırılmış, hizmet sağlanmış ve bir onaylanmış işlem sırası üretmek için, takılabilir bir konsensüs protokolü kullanan servis aşamasına girer. İşlem girdilerini tamamen sipariş eden standart aktif çoğaltmadan farklı olarak, Fabric, işlem çıktılarını yürütme aşamasında hesaplandığı gibi durum bağımlılıklarıyla birleştirir. Her bir eşlenikten sonra, onaylama işlemlerinde onaylama işlemlerinden denetleyici değişikliklerini ve onaylama aşamasında yürütmenin tutarlılığı inceler. Tüm eşler işlemleri aynı sırada onaylarlar ve bu onaylama eylemi deterministiktir. Bir Fabric ağı aslında aynı hizmet servisine bağlı birden fazla Blok Zinciri'ni destekler. Bu tür ağlarda, her bir Blok Zinciri bir kanal olarak adlandırılır ve üyeleri olarak farklı eşleniklere sahip olabilir. Kanal, Blok Zinciri ağının bir bölümü gibi düşünülebilir ancak, kanallar arasında fikir birliği koordine edilmez ve her bir kanaldaki toplam işlem sırası diğerlerinden ayrıdır. Tüm istemcileri güvenilir olarak kabul eden belirli dağıtımlar, eşler için kanallar arası erişim kontrolü de yapabilir (Cachin, 2016).

2.4.2.1. Dağıtma İşlemi

Parametre olarak bir zincir kodunu (akıllı sözleşmeyi), yine zincir kodu olan eşlere kurdurur ve eşleri üzerine yükler.

2.4.2.2. İşlemin Başlaması

Daha önce bir konuşlandırma işlemi ile kurulmuş olan belirli bir zincir kodunun işlemi başlatılır, (argümanlar işlemin türüne özgüdür) duruma göre girişleri okuyabilir, yazabilir ve başarılı veya başarısız olduğunu gösterebilir.

2.4.2.3. Sorgu İşlemi

Her bir zincir kodu, işlem sırasında kendi kalıcı girişlerini tanımlayabilir. Okuma izni verilen bir defterde, işlem uygulandığı için kimlik doğrulama ve yetkilendirme için bir güvenlik altyapısı da bulunur. Açık anahtar sertifikaları aracılığıyla kayıt ve işlem yetkilendirmesini, bant içi şifreleme yoluyla gerçekleşen zincir kodunun gizliliğini destekler. Daha basit bir tabirle, ağa bağlanmak için her eşleniğin üyelik hizmetlerinin bir parçası olan kayıt sisteminden bir kayıt sertifikası alması gerekmektedir. Ağa bağlanmak ve işlem yapabilmek için, gerekli olan işlem sertifikalarını almak ve bir eşleniğe (Peer)

yetki verilmesi elzemdir. Akıllı sözleşmeler için var olan zincir kodu, simetrik anahtar şifrelemesiyle sağlanır ve Blok Zinciri için kayıt sertifikasına sahip tüm eşler için kullanılabilen blok zincire özgü bir anahtarla işlemler yürütülür (Cachin, 2016).

Hyperledger ayrıca; standart ve genel amaçlı programlama dillerinde yazılmış uygulamaları, yerel bir şifreleme ve para birimlerine bağlılık olmadan çalıştıran ilk Blok Zinciri sistemidir. Bu alana özgü dillerde veya kripto para birimlerine güvenilmesi için "Akıllı Sözleşmeler" gerektiren mevcut Blok Zinciri platformlarına böylelikle keskin bir tezat oluşturmaktadır. Her eş, defterin bir kopyasını saklar, eşler hareketleri doğrulamak için, bloklar halinde karma bir zincir oluşturmak amacıyla uzlaşma protokolü yürütürler. Bu süreç tutarlılık için gerekli olduğu gibi işlemleri de istem kabul ederek defteri oluştururlar (Nakamoto, 2008). Açık (Public) veya izinsiz bir zincirde, herkes belirli bir kimlik sahibi olmadan katılım sağlayabilir. Kapalı veya izinli (Private) zincirler ise tipik olarak yerel bir şifreleme para birimi içerir ve genellikle Çalışma İspatı (PoW)'na ve ekonomik teşviklere dayanan fikir birliği kullanırlar. Öte yandan açık blok zincirleri, bilinen ve tanımlanmış bir dizi katılımcı arasında bir Blok Zinciri arasında çalıştırmaktadır. İzinli bir Blok Zinciri, ortak bir amacı olan ancak birbirine güvenmeyen bir grup varlık (Fon, Mal veya Bilgi Alışverişinde Bulunan İşlemler gibi) arasındaki etkileşimi güvence altına almanın bir yolunu sağlar (Androulaki, 2018).

Fabric'in mimarisi, güvenilmeyen bir ortamda güvenilmeyen bir kodun dağıtılması için yeni bir yürütme sırası doğrular. İşlem akışını, sistemdeki farklı varlıklarda da çalıştırabilmek için üç adıma ayırır:

- İşlem yapmak, doğruluğunu kontrol etmek ve onaylamak,
- İşlem semantiğinden bağımsız olarak bir uzlaşma protokolü yoluyla hizmet vermek,
- Eş-zaman nedeniyle zaman ve sonuç koşullarını etkileyebilecek uygulamalara özgü, güven varsayımlarına göre işlem onayı vermek.

Fabric merkezi olmayan veri tabanlarında sıklıkla bulunan pasif ya da birincil yedek kopyalamayı kullanır, ancak ara katman tabanlı asimetrik güncelleme işlemleri ve hata toleransıyla (Byzantine Fault Tolerance) güvenilen ortamlara taşınır. Fabric'te, her işlem yalnızca bir eş alt kümesi tarafından gerçekleştirilir (onaylanır), paralel yürütmeye izin verilir ve potansiyel belirsizlik giderilebilir. Esnek bir onay politikası, belirli bir akıllı sözleşmenin doğru bir şekilde yürütülebilmesi için hangi emsallerin veya kaç tanesinin onaylanması gerektiğini belirler (Miller, 2016).

İkinci olarak, işlemlerin kayıt durumu üzerindeki etkileri, her eşlenik tarafından bireysel olarak yürütülen deterministik doğrulama adımında, ancak aralarındaki toplam istem üzerinde uzlaşmaya varıldıktan sonra yazılır. Bu, Fabric'in işlem onayına göre uygulamaya özgü güven varsayımlarına saygı duymasına olanak verir. Dahası, durum güncellemelerinin sıralaması, fikir birliği için modüler bir bileşen olan atom yayını (Atomic Broadcast)'na devredilir, böylece merkezi olmayan ve mantıksal olarak işlem yürüten ve defteri tutan eşleniklerden ayrıştırılır. Fikir birliği modüler olduğundan, uygulaması belirli bir dağıtımın güven varsayımına göre uygulanabilir. Blok Zinciri eşlerini aynı fikir birliğini uygulamak için de kullanmak mümkün olsa da, iki rolün ayrılması esneklik sağlar ve birinin CFT (Çökmeye hata toleransı) veya BFT (Bizans Hata Toleransı) istemi için iyi kurulmuş araç setlerine güvenmesine izin verir. Genel olarak, hata toleransı modelinde pasif ve aktif replikasyonu birleştiren bu hibrid replikasyon tasarımı ve yürütme-yönetme paradigması, Fabric mimarisindeki temel yeniliği temsil eder ve Fabric'e esnek güven varsayımlarını destekleyen izin verilen bloklar için ölçeklenebilir bir sistem oluşmasında destek olur. Bu mimariyi uygulamak için, Fabric aşağıdaki bileşenlerin her biri için modüler yapı taşlarını içerir (Androulaki, 2018);

- Bir istem servisi atomik olarak denetleyici güncellemelerini yayınlar ve işlemlerin sırası üzerinde fikir birliği kurulmasını sağlar,
- Bir üyelik hizmeti sağlayıcısı, eşleri kriptografik kimliklerle ilişkilendirmekten sorumludur,
- İsteğe bağlı eşler arası bilgi akışı servisi, tüm eşlere servis hizmeti vererek blok üretimini yayar,
- Fabric'te yapılan akıllı sözleşmeler, izolasyon için bir "Konteyner" ortamında gerçekleştirilir,
- Her bir eş, yerel olarak yerel bilgiyi, sadece ekleme bloğu şeklinde ve anahtar değer deposundaki en son durumun anlık görüntüsü olarak saklar.

2.4.3. Blok Zinciri Yürütme Modeli

Tüm önceki blok zincir sistemleri (izinli veya izinsiz) emir-işlem yürütme mimarisini izler. Bu, blok zinciri ağının önce bir uzlaşma protokolü kullanarak işlemleri istem olarak kabul ettiği ve ardından, bunları tüm sıralarda aynı anda yürütmesi anlamına gelir. Mevcut izin verilen blok zincirleri, tipik olarak PBFT (Practical Byzantine Fault Tolerance) için diğer protokoller tarafından sağlanan BFT fikir birliği mekanizmasını

kullanır. Bu esnada, aynı sıra yürütme yaklaşımı ve klasik aktif SMR uygulamasını takip eder.

2.4.3.1. Sıralı Yürütme

İşlemlerin tüm eşler üzerinde art arda yapılması, Blok Zinciri'nin gerçekleştirebileceği etkin verimi sınırlandırır. Bilhassa, iş hacmi uygulama gecikmesi ile ters orantılı olduğu için, bu en basit akıllı sözleşmeler hariç herkes için bir performans darboğazına dönüşebilir. Böyle bir Blok Zincirinin performansını ciddi şekilde azaltan bir hizmet reddi (DoS) saldırısı, uygulanması çok uzun zaman alan akıllı sözleşmelerde tahribata yol açabilir. Örneğin, sonsuz bir döngüyü yürüten akıllı bir sözleşmenin ölümcül bir etkisi vardır, ancak durma sorunu çözülemez olduğu için otomatik olarak algılanamaz. Bu sorunla başa çıkmak için, yürütme, kriptografi temelli halka açık programlanabilir bloklar kullanır.

2.4.3.2. Deterministik Olmayan Kod

Hizmet yürütme mimarisi için bir diğer önemli sorun deterministik olmayan işlemlerdir. Akıllı sözleşmelerin genel amaçlı bir dilde (Örneğin; Go, Java, C/C++) yazılması daha anlaşılır görünmekte ve blok zinciri çözümlerinin benimsenmesini hızlandırmaktadır. Maalesef, genel diller uygulamanın sağlanması için pek çok sorun teşkil etmektedir. Uygulama geliştiriciler açıkça deterministik olmayan işlemler sunmasa bile, gizli uygulama detayları aynı yıkıcı etkiye sahip olabilir. İşleri daha da zorlaştırmak için, bir blok zincirinde, deterministik uygulama yaratma yükü, potansiyel olarak güvenilmeyen programcıya aittir. Kötü niyetle oluşturulan, sadece deterministik olmayan bir sözleşme tüm blok zincirini durma noktasına getirmek için yeterlidir (Cachin, 2016).

2.4.3.3. Uygulama Gizliliği

Denetleyici düğümlerin planına göre, birçok izin verilen sistem tüm eşler üzerindeki akıllı sözleşmeleri yönetmektedir. Bununla birlikte, izin verilen bloklar için amaçlanan birçok kullanım durumu gizlilik gerektirir, yani akıllı sözleşmeler mantığına, işlem verilerine veya defter durumuna erişimin kısıtlanabileceği durumlar için gizlilik protokolü şarttır. Aynı kodu her yerde çalıştırmak yerine, aynı durumu tüm eşlere yaymak yeterlidir. Bu nedenle, akıllı bir sözleşmenin uygulanması, bu göreve güvenilen meslektaşların bir alt kümesi ile sınırlandırılabilir, bu da yürütmenin sonuçları için de geçerlidir. Bu tasarım, aktif taklitten (replikasyon), blok zinciri güven modeline adapte edilmiş bir pasif taklit varsayımına doğru yönelmektedir (Androulaki, 2018).

2.4.4. Yapıya Ek Akıllı Sözleşme

İzin verilen blokların çoğu, fikir birliği oluşturmak için asenkron BFT taklit protokollerine güvenir. Bu tür protokoller tipik olarak n>3f eşlenikleri arasında, f'ye kadar uyumsuz eylem gösteren güvenlik varsayımına dayanırlar. Aynı eşler, genellikle aynı güvenlik varsayımı altında da uygulamalarını yürütürler. Bununla birlikte, bu tür niceliksel bir güven varsayımı, sistemdeki meslektaşların rollerinden bağımsız olarak akıllı sözleşme uygulaması için gereken güvenceyle eşleşmeyebilir. Esnek bir sistemde, uygulama düzeyinde güven, protokol seviyesinde güvenmeye sabitlenmemelidir. Genel amaçlı bir blok zinciri, bu iki varsayımı ayrıştırmalı ve uygulamalar için esnek güven modellerine izin vermelidir.

Takılabilir uzlaşma sistemini tanıtan ilk blok zinciri örneği Fabric'tir. Fabric'ten önce, neredeyse tüm blok zincir sistemleri, izin olsun veya olmasın, kodlanmış bir fikir birliği protokolü ile süregelmiştir. Örneğin, BFT protokolleri, konuşlandırıldıklarında performansları bakımından büyük ölçüde farklılık gösterirler. Zincir iletişim modeline sahip bir protokol, simetrik ve homojen bağlantılara sahip bir LAN kümesinde ispatlanmış bir şekilde optimum verim sergilemektedir ancak; geniş alanlı, heterojen bir ağda bozulmaya uğramaktadır. Ayrıca; yük, ağ parametreleri ve gerçek hatalar veya saldırılar gibi dış koşullar, belirli bir ağ içerisinde zaman içinde değişikliğe uğrayabilir. Bu nedenlerden dolayı, BFT uzlaşma mekanizması doğal olarak yeniden yapılandırılabilir olmalı ve ideal olarak değişen bir ortama dinamik olarak adapte edilmelidir. Bir diğer önemli husus, protokolün güven varsayımını, bir blok zinciri dağıtım senaryosuyla eşleştirmektir.

Daha önce de belirtildiği üzere, Fabric modüler bir blok zincir sistemidir. Özellikle tak-çalıştır özelliğini destekleyen bileşenlerden biri istem hizmetidir. Çoğunlukla sistemi test etmek için kullanılan herhangi bir dağıtık protokol yürütülmeyen merkezi ve çoğaltılmamış bir istem hizmetidir.

2.4.5. Yüksek İşlem Akışı

Yüksek seviye veri akış yürütme aşamasında, kullanıcılar, işlem teklifini (veya basit bir şekilde teklifi) yürütmek için bir veya daha fazla onaylayıcıya imzalar ve gönderirler. Bir teklif, gönderen kullanıcının kimliğini, yapılacak işlem şeklinde işlem yükünü, parametreleri ve zincir kodunun tanımlayıcısını, her kullanıcı tarafından yalnızca bir kez kullanılacak olan bir not ve kullanıcı tanımlayıcısından ve olmayan işlemden

türetilmiş bir işlem tanımlayıcısı içerir. Onaylayıcılar teklifi, Blok Zincirine kurulmuş olan, belirtilen zincir kodunda yürüterek işlemin benzetimi gerçekleştirilir. Zincir kodu ana onay işleminden izole edilmiş bir konteynerde çalışır. Diğer eşlerle senkronizasyon yapılmaksızın, cihaza ait yerel Blok Zinciri durumuna karşı bir teklif benzetimi yapılır. Onaylayıcılar simülasyonun sonuçlarını defter durumuna alamazlar. Blok Zincirinin durumu, işlem yöneticisi tarafından versiyonlanmış bir anahtar-değer deposu biçiminde tutulur. Bir anahtara yapılan art arda güncellemeler monoton olarak artan sürüm numaralarına sahiptir. Bir zincir kod tarafından oluşturulan durum, yalnızca bu zincir koduna dahil edilir ve doğrudan başka bir zincir kodu tarafından erişilemezdir. Uygun görüldüğünde bir zincir kodu, aynı kanal içindeki durumuna erişmek için başka bir zincir kodu çağırabilir. Benzetim sonucu olarak, her bir onaylayıcı, benzetim tarafından üretilen durum güncellemelerini kapsayan, yeni değerleriyle birlikte oluşan bir değer yazma sürecine girmektedir ve aynı zamanda, teklif benzetiminin versiyon bağımlılıklarını temsil eden bir okuma setine de sahip olur. Benzetimden sonra onaylayıcılar, cihazda okunan bir mesajı imzalarlar. İşlem kimliği, onaylayıcı kimliği ve onaylayıcı imzası gibi veriler ile birlikte teklif, kullanıcıya geri gönderilir. Kullanıcı, işlemin çağırdığı zincir kodunun onay politikasını yerine getirinceye kadar onayları toplar. Özellikle, aynı yürütme sonucunu üretmek için politika tarafından belirlenen tüm onaylayıcılar gerekmektedir. Daha sonra, istemci işlemi yaratır ve hizmet servisine iletir (Cachin, 2016).

2.4.6. Doğrulama Aşaması

Bloklar, eşlere doğrudan istem yoluyla iletilir. Yeni bir blok, üç ardışık adımdan oluşan doğrulama aşamasına girer.

- Onay politikası değerlendirmesi, blok içindeki tüm işlemlere paralel olarak gerçekleşir. Değerlendirme, doğrulama sistemi olan zincir kodunun görevidir. Blok zinciri; konfigürasyonunun bir parçası olan ve zincir kodu için yapılandırılmış onay politikasına göre, onayın yapılmasından sorumlu olan statik bir kütüphanedir. Onayın yerine getirilmemesi durumunda, işlem geçersiz olarak işaretlenir ve etkileri dikkate alınmaz.
- Bloktaki tüm işlemler için sırayla okuma-yazma çakışması kontrolü yapılır. Her işlem için, yeniden okuma alanındaki anahtarların sürümleri, defterin şu andaki durumuyla karşılaştırılır ve eşler tarafından yerel olarak depolandıkları ve hala aynı olmalarını sağlar. Sürümler eşleşmezse, işlem geçersiz olarak işaretlenir ve etkileri dikkate alınmaz.

- Defter güncelleme aşaması, bloğun yerel olarak depolanmış deftere eklendiği ve blok zincir durumunun güncellediği son şekilde çalışır. Bilhassa, bloğu deftere eklerken, ilk iki adımda geçerlilik kontrollerinin sonuçları da devam eder. Ayrıca tüm durum güncellemeleri, yazma anahtarındaki tüm anahtar/değer çiftlerini yerel duruma yazarak uygulanır.

3. İNTERNET BANKACILIĞI

3.1. İnternet Bankacılığı Tanımı

İnsan hayatının her alanına giren internet kullanımı büyük bir hızla yaygınlaşırken ticari anlamda kullanımı ve gelişimi 1990 yılından sonra gerçekleşmiştir. Kullanıcı sayısındaki artışla birlikte kullanım alanı artan internet birçok sektörde fayda ve kolaylık sağlamaktadır. Bugün çoğu insanın hayatının vazgeçilmez bir parçası haline gelen internet insan hayatını kolaylaştırmanın yanında büyük avantajlar içermektedir. Günümüzde giyilebilir teknolojiler de bile internetin gücünü kullanmaktadırlar. Dünya genelinde internet kullanıcı sayılarına bakıldığında sürekli bir artış halinde olduğu gözlenmektedir. Dünya nüfusunun 2007 yılında %20,5'inin internet kullandığı tespit edilirken bu miktar çok kısa bir zaman içerisinde iki katına çıkmıştır. Bu oran 2016 yılında %46'ya kadar çıkmıştır. İnternet konusunda yapılan iyileştirmeler, kolaylıklar ve yatırımların sayesinde internete olan bu ilginin artık bu rakamların artacağı söylenebilir. Literatüre bakıldığında internet bankacılığının 1990'lı yılların ortasından sonra uygulanmaya başlandığı görülmüştür. Günümüzde insan hayatının her alanına giren internetin kullanımı gün geçtikçe yaygınlaşma birlikte daha da hızlı bir şekilde ilerlemektedir. Ticari açıdan internet 1990'lı yıllardan sonra gelişmeye ve yaygınlaşmaya başlamıştır (İleri, 2011).

İnternet bankacılığı ise müşterilere sunulan bankacılık hizmetlerinde faydalanılan önemli bir kanal olarak tanımlanabilir. İnternet bankacılığı için bilgisayar önemli bir aracı olarak kabul edilir. Atay ve Apak (2013) bilgisayarı kullanımı kolay ve esnek bir bankacılık aracı olarak ifade etmiştir. İnternet bankacılığı, bankacılık hizmetlerinin bankaların sunduğu uygulamalar sayesinde her hangi bir yerden ve her hangi bir zamanda kullanılan önemli bir dağıtım ve ulaştırma kanalı olmuştur. Bu nedenle daha önce belirtilen internet kullanıcı oranlarına internet bankacılığı kullanan kişilerin oranı da eklenmelidir. Hayatımızın sosyal ve ekonomik açıdan her alanına girmiş olan internet, 25 yıl önce ODTÜ ve TÜBİTAK tarafından başlatılan ve günümüzde bir "proje" kapsamından çıkıp ülke ve insanlar için kalkınma ve büyümenin en önemli unsurlarından biri olmuş, insanların günlük ihtiyacı olan ekmek-su gibi temel ihtiyaçları arasında yerini almıştır.

Gelişim süreci olarak görülen bu 25 yılsonunda Türkiye'de internet kullanıcılarının sayısı 54,3 milyon kişiye çıkmıştır. 2008 yılında yaklaşık olarak 6 milyon olan internet kullanıcı sayısı, 2017 yılı sonu itibariyle 68,9 milyon seviyesine çıkmıştır. 2009 yılında geniş bantın yanında mobil geniş bant hizmetlerinin kullanılmasıyla hem mobil bilgisayar hem cep telefonları sayesinde 2017 yılında bu yolları kullanan internet kullanıcı sayısı 57 milyona ulaşmıştır (Onay ve Ozsoz, 2012). 2016 yılında internet veya elektronik veri alışverişi (EDI) yolu kullanılarak alışveriş yapılma girişimi toplam %10,9'dur. 250 ve üzeri çalışanı olan girişimlerde bu oran %20,9 şeklinde, 50-249 çalışanı olan girişimlerde %12,9 şeklinde ve 10-49 çalışanı olan girişimlerde ise %10,1 şeklinde olduğu belirtilmiştir. Aynı araştırmada "sosyal medya" kullanımı; 10 ve üzeri çalışanı olan girişimlerin 2016 yılında %38,1 iken 2017 yılında %45,7 oranına sahip olduğu ortaya çıkmıştır. Girişimlerin en fazla tercih ettiği sosyal ağlar %95,6 ile sosyal medyadır. Kamu kurum ve kuruluşlarıyla iletişim için 2016'da girişimler %86,2 oranında internet kullanmıştır. Kamu kurum ve kuruluşlarından bilgi almak amaçlı %91,3 oranında, resmi formları edinmek için %78,1, resmi formları doldurmak için %73,2, SGK beyannamesi vermek için %55,8 ve KDV beyannamesi vermek için %53,5 oranında internet kullanmıştır (Demirdöğmez, 2018).

İnternet bankacılığı üzerine araştırmacılar çok fazla konuda çalışma gerçekleştirmişlerdir. Bunlar; internet bankacılığının bankacılık proseslerine uyumu, uygulamanın ülkeye göre ve pazara göre verimi, kullanıcıların tercihleri ve nüfusa göre değişimi, uygulamanın banka performansı üzerine etkisi gibi. Ülkemizde internetin mevduat bankaları şubelerine etkisi adına yürütülen çalışma buna örnektir. Aynı çalışmada internet bankacılığının uyum sürecinde şube karlılığına ve mevduat oranına negatif etkisi olduğu gözlenmiştir fakat şubelerdeki yoğunluğun azalması ve mevcut müşteriyle ilgilenme oranının artması gibi pozitif etkileri de olduğu ortaya çıkmıştır. Bu çalışma kapsamında online bankacılık ve faiz geliri arasında negatif etki de gözlenmiş olup uyum sürecinde oransal analizlerin farklı sonuçlar çıkardığı belirtilmiştir. Faizsiz giderlerin internet bankacılığı kullanımında operasyonel giderlerden daha fazla olduğu belirtilmiştir. Bunun nedeni ise bankaların giderlerinin internet bankacılığında da aynı kalmasıdır. Romanya'da gerçekleştirilen çalışma sonucunda bankalar bu konuda incelenmiş ve çoğunluğunun internet bankacılığına yönelmekten çok daha karışık stratejiler izlediği görülmüştür (Stoica, 2015).

Romanya'da yapılan diğer bir araştırmada Gutu (2014) internet bankacılığına uyumun bankalara kar getireceği ortaya koymuş fakat bu kar miktarlarının bu sektörde önemli miktarlarda olmayacağı belirtilmiştir (Gutu, 2014). Amerika ve Kenya'da yapılan aynı çalışma internet bankacılığının banka performansı üzerinde negatif etki yarattığı da görülmüştür. Karlılık ve İnternet bankacılığı arasında bir ilişki bulunamayan Hindistan'da yapılan diğer bir çalışma da ise bankaların risk profilleri ile internet bankacılığı arasında negatif yönlü bir ilişki ortaya konmuştur (Abubakar vd. 2015). Amerika'da gerçekleşen bir çalışmada internet bankacılı ile yeni kurulan geleneksel bir banka karşılaştırılmış ve buna göre kısa vadede geleneksel bankanın internet bankacılığına göre daha karlı olduğu saptanmıştır. Uzun vadede kapanan farka rağmen geleneksel bankanın kar oranlarının daha önde olduğu belirtilmiştir. Sullivan'ın (2000) ise çalışmalarında tüm bu durumlardan farklı bir sonuç ortaya çıkararak bazı bankalarda giderlerin internet bankacılığında fazla olduğunu ortaya koymuş ancak karlılığın geleneksel bankalardan farklı olmadığı sonucuna ulaşmıştır (Sullivan, 2000).

3.2. İnternet Bankacılığının Gelişimi

1967 senesinde İngiltere'de faaliyet gösteren Barclays Bank tarafından "Cash Dispenser"adı verilen, müşterilerin bankalara gitmeden hesaplarına nakit para yatmasını sağlayan bir uygulama ile dijital bankacılık şekillenmeye başlamıştır. Şimdiki ATM cihazlarına benzer bir yapıya sahip olan bu cihazlar temel bankacılık işlemlerini yapmaya imkan sağlamaktaydı. Teknoloji ile birlikte gelişen bu cihazlar 1983 yılına gelindiğinde yerlerini ATM cihazlarına bırakarak dijital bankacılığın ilk sinyallerini vermesinin başlangıcı olmuştur (Yerlikaya, 2017: 24).

Amerika Birleşik Devletleri'nde geliştirilen altyapı sayesinde bankacılık işlemler telefon aracılığı ile yapılmaya başlanmış; müşteriler işlemlerini şubelere gitmeden evde, ofiste kısaca telefona ulaşabildikleri her yerden yapmaya başlamışlardır. Ancak bu uygulama başarı elde edememiştir. Çünkü insanlar geleneksel bankacılık anlayışından sıyrılamamış, yaptıkları işlem sonucunda fiziki bir belge görmek istemişlerdir. Ayrıca telefon bankacılığı işlemlerinde müşterilerin oluşturdukları şifreleri tuşlamaları gerekmekteydi ama tuşlu telefonlar o dönemlerde pek yaygın değildi (Cronin, 1998). Telefon ile istenilen başarı elde edilemediğinden müşterileri görsel anlamda tatmin edecek televizyon bankacılığı sistemine geçilmiş fakat bu sistemde de gerekli altyapı oluşturulamadığından yine istenilen başarı elde edilememiştir. 1981 yılına gelindiğinde bu altyapı sorunu çözülmüştür, New York'un dört büyük bankası Citibank, Chase Manhattan,

Chemical Bank ve Manufacturers Hanover bir araya gelerek "Videotex" adlı sistemi geliştirmişlerdir. Bu sistem; klavye ve ekrandan oluşan bir makine ile uygulanmaya başlanmıştır. Müşteri ve banka bu uygulama ile görsel olarak iletişime geçerek bankacılık işlemlerini gerçekleştirmişlerdir. Ancak bu sistemin fazla maliyetli olması dolayısıyla istenilen geri dönüş elde edilememiştir (Yücel, 2012).

Videotex ile istediği verimi elde edemeyen Chemical Bank, 1983 yılnda geliştirdiği "Pronto" adlı sistemle müşteriler ile kişisel bilgisayarları aracılığı ile temasa geçmeyi amaçlamıştır. 1985 de AT&T ile bir ortaklık kurarak "Covidea" adı altında ev/ofis bankacılığı hizmeti sunmaya devam etmiştir. Ancak yine maliyetleri minimize edemediği için 1989 da bu uygulamayı da terk etmek zorunda kalmıştır. Banka ile müşterilerin evlerinde birbiri ile bağlantılı bilgisayar sistemleri kurularak, müşterilerin banka hesaplarına ulaşımını sağlayan bir sistemdir. Müşteriler, ev ve işyerlerinde bulunan televizyon ve bilgisayarlar aracılığı ile banka hesaplarını kontrol etmekte, virman işlemleri yapmakta ve bankalara talimatlar vermekteydi. Müşteriler kişisel bilgisayarları ve modem cihazları vasıtasıyla, telefon hatlarını kullanarak banka bilgisayarları ile iletişim sağlamaktaydı. Böylece müşteriler şubelerine gitmeden bankacılık işlemlerini evlerinden ve işyerlerinden yapabilmekteydi (Horvitz, 1996).

1900'lerin sonlarına doğru, bankacılık sistemi teknolojinin değişmesi ve gelişmesi, nüfus özelliklerinin değişmesi ve müşteri ihtiyaçlarının artması gibi etmenlere kayıtsız kalamayıp elektronik bankacılık sistemine yönelmiştir. Geleneksel bankacılık sisteminin kağıt dokümanlara bağlı olarak işlemesi, personele ve mesai saatlerine bağımlı bankacılık hizmetleri sunması, bankalara hem evrak takibinde ve saklanmasında zorluk çekmesi hem de personel giderlerinin artması olarak yansımıştır. Günümüzdeki internet bankacılığının temelleri 1990'lı yılların başlarında atılmaya başlamıştır. Bunun temel nedenleri; kişisel bilgisayarların artık o kadar da maliyetli olmamasından dolayı hemen hemen her eve girmeye başlaması, internet altyapısının iyileştirilerek erişim hızının artırılması, insanların internet kullanımına sıcak bakmaya başlamasıdır. Şu an kullanmakta olduğumuz internet bankacılığının ilk örneği 1994 senesinde Amerika Birleşik Devletleri'nde bulunan Stanford Federal Credit Union firması tarafından oluşturulmuştur. Çoğu banka geleneksel bankacılık hizmetlerinin yanında dijital bankacılık hizmetleri vermektedir. Ancak 20. YY'ın sonlarına doğru bankacılık hizmetlerini yalnızca dijital olarak sunan bankalar kurulmaya başlamıştır. 2002 yılı verilerine bakıldığında ABD'de 8 bankanın toplam 1 milyon internet bankacılığı kullanıcısı müşterisi vardı. 2005 yılında internet bankacılığı

kullanımı artarken güvenlik sorunlarını da beraberinde getirmiştir. İnternet korsanları banka müşterilerinin hesaplarına erişip paralarını çalmaya başlamıştı. FFIEC (Federal Financial Institutions Examination Council) bu güvenlik açığını önlemek amacıyla yeni kurallar duyurdu. Bu kurallara göre bankalar müşterilerini internet bankacılığı hakkında bilgilendirmeli ve bazı güvenlik ölçütleri kullanmalıydı. Tabii o dönemdeki güvenlik önlemleri günümüz teknolojisiyle kıyaslanamaz. Günümüzde genellikle iki aşamalı güvenlik önlemleri kullanılmaktadır. İnternet bankacılığı kullanıcısı hesabına erişmek için öncelikle kendi belirlediği şifreyi girerken ikinci aşamada bankanın profilinde kayıtlı olan telefon numarasına gelen şifreyi girerek hesabına giriş yapmaktadır. Bu önlemler sayesinde kötü niyetli internet korsanlarının internet üzerinden diğer insanların hesap bilgilerine ulaşması az da olsa engellenmeye başlanmıştır. ING ve HSBC gibi büyük bankalar "Direct Bank" (geleneksel şube bankacılığında bulunan fiziki şubeler olmadan) adlı bir bankacılık hizmeti sunarak, bankacılık hizmetleri erişimine daha rahat ulaşılmasını sağlamışlardır. Bu sistem günümüzde halen kullanılmaktadır. "Mint.com" en kullanışlı ve şık tasarımlı ara yüz sistemiyle bir çok müşterinin internet bankacılığına erişimini sağlamıştır.

2007 senesine gelindiğinde Apple şirketi ilk Iphone'u piyasaya sürdü. Böylece mobil bankacılık hayatımıza hızlı bir şekilde giriş yaptı. Mobil bankacılık, müşterilerin bankalara gitmesine gerek kalmadan veya ebatça büyük olan tablet veya bilgisayarlara gerek kalmadan bankacılık hizmetlerine ulaşmasını sağlayan "cep bankacılığı"dır. Bankalar da müşterilerin mobil bankacılığı geleneksel bankacılığa tercih ettiğini fark ederek yatırımlarını bu alana kanalize etmişlerdir. Örneğin ülkemizde bulunan Yapı Kredi Bankası dünyadaki on binlerce bankayı geride bırakarak ve Global Finance tarafından "Dünyanın En Yenilikçi Dijital Bankası" seçilmiştir. 2009 yılında ABD'de 54 milyon kişi bankacılık işlemlerini internet üzerinden yürütmekteydi. Bu yüzden pek çok banka geleneksel bankacılık sistemini terk ederek şubelerini kapatmaya başladı. Örneğin 1970'te Amerika'da bulunan banka şubesi sayısı 9340 iken 2009 senesine gelindiğinde bu sayı 3684'e düşmüştür (Tekeli, 2015).

Global antivirüs yazılım kuruluşu ESET'in 2015 senesinde, çeşitli ülkelerde internet bankacılığı kullanımı üzerine bir araştırma yaparak internet bankacılığı kullanıcı sayılarını ölçmeyi amaçlamıştır. Bulgulara göre teknoloji öncüsü Almanların yüzde 70'i internet bankacılığından uzak duruyor. Almanların sadece yüzde 30'u online bankacılıktan faydalanırken, İngilizlerin yüzde 60'ı, Amerikalıların yüzde 54'ü, Rusların ise yüzde 72'si internet bankacılığını kullanıyor. Dünya geneline baktığımızda ise mobil bankacılığı

kullanan kişi sayısının 2020'ye kadar 2 milyar kişiye ulaşması bekleniyor. Juniper Research'ün hazırladığı rapora göre bankaların mobil uygulamalarının büyüme grafiği 2020'ye dek devam edecek. Bankalar ise teknolojik gelişmelere paralel olarak kullanıcıların ihtiyaçlarına ve deneyimlerine göre daha iyi hedeflenmiş ve daha çok ilgili seçenekler sunmaya devam edecek. Bunun en önemli sebeplerinden biri olarak da bankaların diğer marka ve şirketlere göre mobil teknolojiye daha fazla teknoloji yatırımı yapması olarak gösterilmektedir (Horvitz, 1996).

Gün geçtikçe bankalar ve müşteriler geleneksel bankacılık anlayışını terk ederek, dijital bankacılığa yönelmişlerdir. Temmuz-Eylül 2017 dönemi içinde aktif bireysel dijital bankacılık müşterilerin yaş grupları bazında dağılımında ilk sırayı yaklaşık 11 milyon 414 bin kişi ile 36-55 yaş grubu almaktadır. Bunu, 10 milyon 478 bin kişi ile 26-35 yaş grubu, 6 milyon 673 bin kişi ile 18-25 yaş grubu izlemektedir. 56- 65 yaş grubundaki aktif bireysel dijital bankacılık müşteri sayısı ise 1 milyon 523 bin kişidir. Temmuz-Eylül 2017 dönemi içinde toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısı 32 milyon 186 bin kişidir. Bu sayının yaklaşık 5,7 milyon kişisi "sadece internet bankacılığı" işlemi yaparken 19,4 milyon kişisi "sadece mobil bankacılık" işlemi yapmıştır. Hem internet hem mobil bankacılık işlemi yapan kullanıcı sayısı ise 7,1 milyon kişidir. Toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısında bir önceki döneme göre 1 milyon 539 bin kişi artmıştır.

Türkiye'nin internet bankacılığı ile tanışması ise Türkiye'nin ilk özel bankası olan Türkiye İş Bankası aracılığı ile olmuştur. Türkiye İş Bankası 1987 yılında elektronik bankacılığın temeli olan ATM (Automatic Teller Machine) kullanımını başlatmıştır (Polatoğlu ve Ekin, 2001). ATM cihazları, banka tarafından müşterilere verilen plastik bir kart ile neredeyse şubeden yapılabilecek tüm bankacılık işlemlerinin yapılmasına yarar. Günümüzde ATM'lerde plastik kartlar haricinde, parmak izi, avuç içi izi, telefon kamerasıyla barkod okuma, telefona banka tarafından gönderilen mesaj aracılığı ile ve bluetooth teknolojisi gibi pek çok yolla işlem yapılabilmektedir. ATM cihazlarından sonra bankacılık hizmetlerinde yapılan en önemli ikinci hizmet olarak telefon bankacılığı hayatımıza girmiştir. Bankalar tarafından oluşturulan çağrı merkezleri aracılığıyla müşteriler hesaplarına ulaşabilmektedir. Telefon bankacılığından sonra bankacılık sisteminde çığır açan bir diğer olay da internet bankacılığıdır. ATM cihazlarında olduğu gibi internet bankacılığını da ülkemize getiren banka, Türkiye'nin ilk özel bankası olan; Türkiye İş Bankası'dır. 1997 senesinin Haziran ayında internet bankacılığını müşterilerin

hizmetine sunan Türkiye İş Bankası'nı temmuz ayında Garanti Bankası takip etmiştir (Ortunç, 2003).

Türkiye İş Bankası'nda sonra Garanti Bankası, Osmanlı Bankası, Pamukbank, Esbank, Akbank ve Yapı Kredi bankaları da internet bankacılığı hizmetini kullanmaya başlamışlardır. Günümüzde de bankalar internet bankacılığı hizmetlerini geliştirerek hala müşterilerine hizmet vermektedirler. Türkiye Ticaret Bankaları, internet bankacılığını 1997'den bu yana müşterilerin hızlı, etkili ve kolay hizmet almak istemeleri, bilgisayar kullanımının artması, bankacılık ve finans sektöründeki düzenlemelere dayanarak bir dağıtım kanalı olarak kabul etmektedir. Ancak müşteriler hala kafalarındaki soru işaretlerini ve internete olan güven duygularını yenemedikleri için internet bankacılığı kullanımına sıcak bakmamaktadırlar. Türkiye Bankalar Birliği'nin yayınladığı "İnternet ve Mobil Bankacılık İstatistikleri Mart 2016" raporuna göre İnternet bankacılığı yapmak üzere sistemde kayıtlı olan ve en az bir kez giriş işlemi yapmış toplam bireysel müşteri sayısı Mart 2016 itibariyle, 45 milyon 701 bin kişi olmuştur. Son bir yıl içerisinde en az bir kez giriş işlemi yapmış toplam bireysel müşteri sayısı ise 24 milyon 905 bin kişidir. Ocak-Mart 2016 döneminde 17 milyon bireysel müşteri en az bir kez internet bankacılığı giriş işlemi yapmıştır. Bu miktar, toplam kayıtlı bireysel müşteri sayısının yüzde 38'ini oluşturmaktadır. Aktif bireysel dijital bankacılık müşterilerinin 23 milyon 415 bin kişisi erkek (yüzde 70), 9 milyon 959 bin kişisi kadın (yüzde 30) müşterilerdir. Ekim-Aralık 2017 dönemi içinde aktif bireysel dijital bankacılık müşterilerin yaş grupları bazında dağılımında ilk sırayı yaklaşık 12 milyon 273 bin kişi ile 36-55 yaş grubu almaktadır. Bunu, 11 milyon 117 bin kişi ile 26-35 yaş grubu, 7 milyon 542 bin kişi ile 18-25 yaş grubu izlemektedir. 56-65 yaş grubundaki aktif bireysel dijital bankacılık müşteri sayısı ise 1 milyon 692 bin kişidir. Ekim-Aralık 2017 dönemi içinde toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısı 34 milyon 990 bin kişidir. Bu sayının yaklaşık 5,5 milyon kişisi "sadece internet bankacılığı" işlemi yaparken yaklaşık 22 milyonu "sadece mobil bankacılık" işlemi yapmıştır. Hem internet hem mobil bankacılık işlemi yapan kullanıcı sayısı ise 7 milyon 676 bin kişidir. Toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısında bir önceki döneme göre 2 milyon 804 bin kişi artış olmuştur.

3.3. İnternet Bankacılığının Sağladığı Faydalar

İnternet bankacılığı kullanımının artmasının, alışılagelmiş bankacılık kanallarına kıyasla pek çok faydası vardır. Müşteri odaklılığını ve memnuniyetini sağlamak, maliyetleri düşürmek, yeni ve çeşitli ürünlerin sunulmasına yardımcı olmak, satışları ve

müşteriyle etkileşimi kolaylaştırarak daha fazla sayıda müşteriye ulaşmak, coğrafi bölgeyle ve zamanla kısıtlı kalınmadan hizmet sunabilmek bu avantajlara örnektir. Ek olarak, internet bankacılığının diğer faydaları, bankalar açısından şube sayısının azaltılması, daha az personel istihdam edilmesi, hizmet ve reklam maliyetlerinin azaltılması, kira, kırtasiye masrafları ve diğer giderlerin düşürülmesidir (Yurttadur ve Süzen, 2016). İnternet bankacılığının bankalara sağladığı diğer faydalar arasında, marka imajının güçlendirilmesi, müşteri sayısının artırılması böylece daha fazla satış imkanı sağlanması, mevcut müşterilerle ise yenilikçi hizmetler yoluyla çalışmaya devam edilmesi, müşteri sadakatinin arttırılması ve sunulan hizmetlerin iyileştirilmesi, sektördeki yeniliklere hızlıca adapte olarak stratejik üstünlük sağlanması, daha az maliyetle işlem olanağı elde edilmesi ve şubelerde yaşanan yoğunluğun azaltılması şeklinde sıralanabilir. Müşteriler açısından bakıldığında internet bankacılığına herhangi bir yerden herhangi bir zamanda şubelere göre daha az masrafla ulaşılabilir. Bankaların müşterilerini internet bankacılığı kullanımına teşvik etmesi de burada bir etkendir. İnternet bankacılığıyla bireyler haftanın her gününde ve günün her saatinde ihtiyaç duydukları hizmetleri banka çalışanlarının bile görmemesi sebebiyle, gizlilik ve güvenlik kuralları dahilinde gerçekleştirebilecek, banka şubelerindeki zaman kayıpları engellenecektir. Ayrıca firmalar, ihtiyaçlar doğrultusunda kişisel yetkilendirme ve onay sistemi de talep edebilecektir. Bu sayede, kullanışlı ve güvenilir bir otokontrol sistemi sağlanabilmektedir. Banka sistemlerindeki sayısallaşma oranı arttıkça bankalar tüketicilerinin ihtiyaçlarına cevap verebilmek için daha fazla zaman ayırabilecekler ve böylece tüketici memnuniyetinin izlenmesi, tüketicilerden daha fazla geri besleme alınması ve tüketicilere özgü çözümler üretilmesi imkanı elde edeceklerdir (Eroğlu ve Yücel, 2012).

Müşterilerin internet bankacılığını benimsemesinde etkili olan bazı faktörler; diğer kanallara kıyasla daha faydalı olduğunun düşünülmesi, kişilerin çalışma zamanlarına uygun olması, güvenlik-gizlilik veya risk faktörleri, internet işlemlerinde olan deneyimleri, kolay ulaşılabilen bir bankacılık kanalına duyulan gereksinim ve teknolojik yeniliklerle ilgili becerileri şeklinde belirtilmiştir. Faydalarının yanı sıra internet bankacılığının bazı dezavantajları da mevcuttur. İnternet bankacılığı kullanımını anlamak yeni başlayanlar için ilk başta zor olabilir. Çevrimiçi hesaplara nasıl erişileceği üzerine demo sunan bazı siteler olsa da, tüm bankalar bu imkânı sunmuyor. İnternet bağlantısı yoksa çevrimiçi bankacılık hizmetlerine erişilemez. İnternet bağlantısının kopması veya yavaş bağlantı nedeniyle bazen işlemlerin gerçekleşip gerçekleşmediğini anlamanın zorlaşması diğer bir sorundur.

İnternet bankacılığında karşımıza çıkan en büyük problem hiç kuşkusuz ki güvenlik sorunudur. İnternette yayılan bilgisayar virüsleri ile kötü amaçlı kişiler tarafından dosyalar, elektronik posta ve internet bankacılığı şifreleri kişilerin bilgisayarından veya internet üzerindeki hesaplarından çalınabilir. Buna inanan internet kullanıcıları, interneti muhtemelen ticari amaçlarla kullanmayacaktır. Bu gibi risklere karşı kişiler gördüğü reklamlara da güvensiz bulduğu için tıklamamaktadır. Bu açıdan reklamlar başarılı olsa dahi kişilerin bankayı kullanmalarını sağlayamadığı için hedefe ulaşamamaktadır (Akın, 2007).

3.4. İnternet Bankacılığı Araçları

Teknoloji geliştikçe kişiler ve kurumlar çağa ayak uydurarak tüm işlerini hızlı, basit ve sorunsuz şekilde yapmak istemektedirler. Çağı yakalamak her zaman bir adım önde olmak demektir. İletişim sektörünün her zaman güncel teknolojiyi takip etmesi, bilginin daima ulaşılabilir olmasını sağlamaktadır. İnternetin gelişmesiyle beraber günlük yaptığımız hemen hemen her işlem elektronik ortama taşınmıştır; e-okul, eposta, e-devlet, e-ticaret gibi. Bankacılık sektörü de bu durumdan etkilenerek e-bankacılığa hızlı bir geçiş yapmıştır. Elektronik bankacılık, bankacılık hizmetlerine ulaşmamız için bizi herhangi bir mekana, herhangi bir saat dilimine bağlı kılmamaktadır (Yazıcı, 2004).

Elektronik bankacılık, geleneksel bankacılık yöntemlerine bağlı kalmadan bankacılık hizmetlerinden yararlanmayı sağlamaktadır. Türkiye'de faaliyet gösteren bankalar 20. Yüzyılın son çeyreğinde ülke dışına açılmaya başlamıştır. Sundukları hizmetlerin kalitesini artırarak tam rekabet piyasasında tutunmayı amaçlayan bankalar, bu konuda bilgi teknolojilerinden yararlanarak yatırımlarını bu yönde kanalize etmişlerdir. Türkiye'nin geleneksel bankacılıktan şubesiz bankacılığa geçici 1900'lü yılların ilk yarısında olmuştur. Bilgi teknolojisi araçları olan bilgisayar ve iletişim araçlarının yardımı ile bankacılık hizmetlerinin çeşitliliği, niteliği artarak bankaların hizmet algısında büyük bir değişikliğe gitmesini sağlamıştır. Basel Bankacılık Denetim Komitesi'nin, elektronik kanallar aracılığıyla bankacılık ürün ve hizmetlerinin sağlanması olarak tanımladığı, elektronik bankacılık hakkında üç yayımı vardır (Bayoğlu, 2010).

- 20 Mart 1998, Elektronik Bankacılık ve Elektronik Para Faaliyetleri İçin Risk Yönetimi,
- Elektronik Bankacılığa İlişkin Risk Yönetimi İlkeleri, 17 Temmuz 2003,
- Ağustos 2003, Sınır Ötesi Bankacılık Faaliyetlerinin Yönetimi ve Denetimi.

Teknoloji ve bankacılık hizmetlerinin entegre olması ile birlikte birçok elektronik bankacılık ürünü bankalar tarafından kullanıma sunulmuştur. İnternet bankacılığı, teknolojinin gelişmesiyle beraber hayatımıza girmiş bir alternatif dağıtım kanalı ve elektronik bankacılık ürünüdür. İnternet bankacılığı tüm elektronik bankacılık ürünleri sonunda ayrı bir bölüm olarak ele alınacaktır.

3.4.1. Nakit Yönetimi

Nakit; para veya vadesiz mevduat demektir. Nakit yönetimi ise, nakit fazlası ve açıklarına neden olmadan işletmede bulundurulmasını gerektiren etkin düzeydeki para miktarını ifade etmektedir. İşletmenin kasasında bulundurması gereken tutar, ödeme ve alacaklar dengesini kurarak belirlenir. Hayatımıza hızlı ve etkili bir giriş yapan internet, ticari hayatın da vazgeçilmez bir parçası olmuştur. Rakiplerinin önüne geçmek isteyen her firma, teknolojik gelişmeleri yakından takip etme ve kendini çağa uydurma ilkesini benimsemelidir. İnternet ortamında zaman ve mekan kavramı olmadığı için ticari anlamda öne çıkan sorunların çoğu ortadan kalkmıştır. Firmalar online alışveriş siteleri kurarak, diğer firmaların kurduğu sitelerdeki ürün ve fiyat listelerinden kendi sitesi ile karşılaştırarak, piyasaya hakim olabilir ve stratejilerini belirleyebilmektedirler. Ayrıca müşteriler de, dünyanın neresinde ve saat kaçta olursa olsunlar, firmaların ürünlerini ve hizmetlerini inceleyerek, sipariş verebilir ve ödeme işlemlerini de gerçekleştirerek, diledikleri ürün veya hizmete sahip olabilirler. Bu sayede internet üzerinden satış yapma sisteminde de rekabet arttığı için sunulan malın kalitesi artacak ve uygun fiyat seçenekleri çoğalacaktır. İnternet üzerinden online satış yapan firmaların ve alışveriş yapan müşterilerin önem verdiği unsurlardan biri de para transferlerinin güvenilir, hızlı ve doğru bir şekilde yapılmasıdır. Bu noktada da bankalar devreye girmektedir. Dünya üzerinde pek çok kez ekonomik krizler yaşanmıştır. Bunlardan en yakın tarihlisi de 2008 dünya ekonomik krizidir. Enerji ve petrol fiyatları düşmüş, arz-talep arasında büyük bir fark oluşmuş ve enflasyonun düşüşe geçmesine neden olacak daha pek çok ekonomik unsur etkili olmuştur. 2011 yılında Avrupa ülkelerinde yaşanan borç krizinden yine tüm dünya olumsuz etkilenerek bir kriz başlamış, bu nedenle merkez bankaları faizleri düşürme yoluna gitmişlerdir. Bankacılık sektörü de bu krizden en az düzeyde etkilenmek için verimliliği artırma, operasyonel işlemlerin maliyetini düşürme gibi yöntemlere başvurmuşlardır. Bu stratejiyi uygularken de en etkili yöntem olarak internet bankacılığı ve alternatif dağıtım kanalları (ADK) seçilmiştir. Zaman ve mekandan bağımsız olarak

bankacılık işlemlerinin gerçekleşmesini sağlayan internet bankacılığı, alternatif bir dağıtım kanalıdır (Altınışık, 2000).

ING Bank, Türkiye dahil 13 Avrupa ülkesinin yanı sıra ABD ve Avustralya'da gerçekleştirdiği Mobil Bankacılık 2016 Raporu'nun sonuçlarına göre mobil bankacılığın nakit yönetimine olumlu etkisi en çok Türkiye'de kendini gösteriyor. ING Bank'ın 15 bine yakın katılımcıyla gerçekleştirdiği araştırmadan öne çıkanlar özetle şöyle: Avrupalı tüketiciler arasında mobil bankacılık kullanım oranı yüzde 41'lik seviyesinden yüzde 47'ye çıktı. Yüzde 16'lık kesim de önümüzdeki bir yıl içinde mobil bankacılığa geçmeyi düşünüyor. Türkiye ise mobil bankacılıkta yüzde 44'lük aktif kullanım ve yüzde 15'lik bir yıl içinde yeni kullanım beklentisine sahip. Avrupa'daki mobil cihaz sahiplerinin yüzde 66'sı son 12 ay içinde en az bir kez mutlaka mobil alışveriş yapmış. Katılımcıların yüzde 85'i, gelecek 12 ay içinde daha az nakit kullanacağını belirtiyor. Amerikalıların yüzde 78'i ve Avrupalıların yüzde 71'i mobil bankacılığın nakit yönetimine olumlu etkisi olduğuna inanırken, bu konuda en iyimser ülke Türkiye. Türkiye'deki tüketiciler arasında bu oran yüzde 85. Katılımcıların yüzde 23'ü mobil bankacılık sayesinde hiçbir fatura ödemesini kaçırmadıklarını, yüzde 16'sı ise mobil çözümler sayesinde daha fazla tasarruf yapabildiklerini ifade ediyor. Tüketicilerin mobil bankacılık kanallarını günlük bazda ne kadar sıklıkta kullandıklarını konusunda ise sıralama şu şekilde: Yüzde 19 ile internet bankacılığı yüzde 12 ile mobil bankacılık ve yüzde 5 ile ATM'ler. Mobil cihazlardan 2015'te ve 2016'da yapılan alışverişler incelendiğinde Avrupa ortalaması yüzde 58'den yüzde 66'ya yükseldi. Türkiye mobil alışverişteki liderliğini korurken; geçen yıl yüzde 84 olan oran bu yıl yüzde 88'e çıkmıştır.

3.4.2. Akıllı Kartlar

İlk kez 1970'lerin başında Fransa'da telefon kartlarında akıllı kart özelliği kullanılmaya başlanmıştır. Avrupa ve ABD kimliklerde, sağlık kartlarında, mobil telefonların SIM kartlarında ve kredi kartlarında kullanılarak akıllı kart sitemini geliştirmiştir (Kara, 2002). Ülkemizde 2008'e kadar çipsiz, manyetik bantlı kartlar kullanılmıştır. Manyetik alan üzerinde kullanıcıların; adı-soyadı, şifre bilgisi, hesap bilgileri gibi temel unsurlar yer almaktaydı ve kullanıcı imza atarak işleme onay vermekteydi. Ancak bu manyetik alanın yetersiz olmasından dolayı çoğu bilgi depolanamamaktaydı ve buradaki bilgiler kolayca kopyalanabilmekteydi. Bu yüzden kartlara çip özelliği getirilerek bilgi depolama alanı ve güvenlik önlemleri artırılmış oldu. Akıllı kartlar oldukça gelişmiş bir güvenlik sistemine sahiptirler. Kart bilgilerinin başkaları

tarafından kopyalanması oldukça zor ve kartın alacağı fiziki darbelere karşı dayanıklı olması akıllı kartların temel özelliklerindendir (Yılmaz, 1999).

3.4.3. Elektronik Cüzdan

Teknolojinin gelişmesiyle doğru orantılı olarak bankacılık sektörü de gelişmiştir. Bankalar, online alışveriş sitelerini kullanan müşterileri için bir elektronik cüzdan uygulamasını geliştirmişlerdir. Bu uygulama mobil cihazlarla uyumlu olarak kullanıcıların banka bilgileri ile entegre çalışmaktadır. Kullanıcıların bilgileri bir defalığa mahsus olmak üzere tanımlanarak, internet alışverişlerinde bu bilgiler kullanılmaktadır (Yücel, 2012).

3.4.4. Elektronik Para

Elektronik para ihraç eden kuruluş tarafından kabul gören fon karşılığı ihraç edilen, elektronik olarak saklanan bir değerdir. Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değerdir.

3.4.5. Kredi Kartları

Nakit para yerine geçecek olan ilk kredi kartı 1950'de Dinners Club tarafından çıkarılmıştır ve kısa zaman içinde Amerika'da yaygınlaşmıştır. Ülkemize kredi kartının girişi 1968'de Dinner Club ve American Express aracılığı ile sağlanmıştır. 1980lerin başında ülkemizde yaygın olarak kullanılmaya başlanmıştır. 1990'da Bankalar arası Kart Merkezi'nin kurulmasıyla kredi kartı kullanımı ülke geneline yayılmaya başlanmıştır (Erdem ve Efiloğlu, 2002). Bankalar Arası Kart merkezi verilerine göre, 2015 yılı Mart ayı kartlı ödeme verilerini açıkladı. BKM açıklamasına göre; Mart ayı sonunda Türkiye'de 108 milyon banka kartı ve 58 milyon kredi kartı bulunmaktadır. 2014 yılı Mart ayı ile kıyaslandığında banka kartındaki %6'lık artışa karşın kredi kartı sayısının neredeyse artmadığı görülmektedir. Son 12 ayda 200 bin adet artan kredi kartı sayısı 58 milyona yeni ulaşmıştır (Yücel, 2012).

3.4.6. Sanal Kredi Kart

Sanal Kart ile tüm yurt içi ve yurt dışı internet sitelerinden güvenle ve kolaylıkla alışveriş yapabilir. Fiziki kredi kartına bağlı olarak çalışan, kartın fiziki olarak bulunmadığı ve dolayısıyla kayıp/çalıntı riski taşımayan, internet ve mail order alışverişlerinizde kullanılabilen bir kredi kartıdır.

3.4.7. Akıllı Anahtarlar

Akıllı anahtar sistemi ikili güvenlik aşamasından oluşur. İnternet bankacılığına giriş şifresinin yanı sıra akıllı anahtarların oluşturduğu 8 haneli şifre kullanılır ve bu şifre her seferinde değişir.

3.4.8. SWIFT

Yurt içi ve yurt dışındaki bankalara döviz transferi işlemlerinin kolayca gerçekleştirmeye yarayan bir sistemdir. Her bankanın kendine ait bir SWIFT kodu vardır. Banka Swift kodları 11 haneden oluşur. Eğer Swift kodu 11 haneden az ise, sonuna X harfi ekleyerek 11 haneye tamamlanmalıdır.

3.5. İnternet Bankacılığı Türleri

İnternet bankacılığının iki türü vardır. Bunlar bireysel internet bankacılığı ve kurumsal internet bankacılığıdır.

3.5.1. Bireysel İnternet Bankacılığı

İnternet bankacılığında, bir banka personeline gerek kalmaksızın müşteri, kendi talimatları doğrultusunda otomatik olarak işlemlerini gerçekleştirebilmektedir. İnternet kullanımının günden güne yaygınlaşmasıyla bu kanaldan gerçekleştirilen banka işlem sayısında gittikçe artış sağlanmaktadır. Bu kanaldan yapılabilen başlıca işlemler; hesap bilgileri görüntüleme, vadeli ve vadesiz hesap açılışı, günlük işlem listesi ve hesap hareketleri görüntüleme, banka kartı başvurusu yapmak, kart bilgilerine ulaşabilme, kredi kartı ekstresi, nakit avans başvurusu, kredi kartı borç ödeme işlemleri, havale, EFT gibi para transferleri yapmak olarak sıralanabilir. Ayrıca EFT iptalleri veya durumunun takip edilmesi, düzenli ödeme talimatı oluşturma, yatırım fonu alma, altın, bono, tahvil, pay senedi, döviz, vadeli işlem ve opsiyon borsası, repo, halka arz, hazine ihalesi ve benzeri işlemleri yapabilme, kredi başvurusu izleme, fatura ödeme, faturasız hat TL yükleme, SGK ve vergi işlemleri, otomatik geçiş sistemi (OGS), hızlı geçiş sistemi (HGS) işlemleri, şans oyunları, bağış işlemleri, poliçe veya bireysel emeklilik görüntüleme, şifre işlemleri, kullanım ayarlarını kişiselleştirme yapılabilen diğer işlemlerdir.

İnternet bankacılığı, şube maliyetleri dolayısıyla azalan kârlılığa çözüm arayan bankalar açısından iyi bir gelir kaynağı rolündedir. Günümüzde genellikle işlemlerin kolayca yapılabilmesinden dolayı talep gören bu kanala ilk başta kapsamlı bir teknolojik altyapı gereklidir. Fakat elektronik bankacılık kanalının şubelere kıyasla maliyetleri az olduğu için az bir zaman zarfında kazanım sağlanabilir. Bu açıdan verimlilik ön plandadır.

Şubede yapılan bir işlemin internet veya cep bankacılığa kıyasla yaklaşık 15 kat maliyeti bulunur. Ayrıca teknolojik yatırımların maliyetli olmasına rağmen bir defa bu altyapı sağlanınca kolayca tasarrufa geçilebiliyor. Dolayısıyla bankacılık sisteminde bu kanalların önemli yeri vardır. Günümüzde bankalar kullanıcılara ATM, telefon ve internet bankacılığı yoluyla verdiği hizmetlerle günlük işlem yoğunluğunu azaltmaya çalışmaktadırlar. Bu kanalların banka ve müşteriler açısından çeşitli artıları vardır. Bunlar, işlemlerin nispeten az masraflara sahip olması, kişilerin bu hizmete yönlendirilmesini sağlayarak şubedeki kalabalığın önüne geçilmesi ve maliyetlerin azaltılmasıdır (Yılmaz, 1999).

3.5.2. Kurumsal İnternet Bankacılığı

Kurumsal internet bankacılığı banka nezdinde bulunan hesaplara güvenli bir ortamda ulaşarak istenilen yerden bankacılık işlemleri yapılmasını sağlar. Bireysel internet bankacılığında olduğu gibi 7/24 bütün işlemler yapılabilir. Şube kanalıyla yapılabilecek pek çok işlem, daha düşük masrafla gerçekleştirebilir. Kurumsal internet şubesinde istenildiği kadar alt kullanıcı belirlenip yetki tanımlamaları yapılabilir. Yetki düzeyleri sıralanıp özelleştirilebildiği gibi onay işlemlerinin nasıl yapılabileceği alt kullanıcılar düzeyinde işlem ve limit bazında belirlenebilir. Tanımlanan kullanıcılar için istenilen sınırlamalar getirilebilir. Banka şubesine veya belirlenen diğer alt kullanıcılara yetki aktarımı yapılabilir. Firmalar kendi alt firmalarına ait hesapları internet bankacılığı hesaplarından izleyebilir. Kurumsal internet bankacılığından yapılabilen işlemlerden bazıları; hesap bilgilerine ulaşma, vadesiz veya vadeli hesap açmak ve kapatmak, vadesiz döviz hesabı açma, vadeli hesap faiz tutarı çekme, yatırım hesabı açma, çek bilgileri görüntüleme, dekont işlemleri, hesap adı tanımlama, ana hesap tanımlama, kredi kayıt bürosu risk raporu, hesaplar arası para transferleri, yatırım transfer işlemleri, döviz transferi işlemleri, kredi kartı işlemleri ve benzeri sayılabilir. Ticari kurumlar internet bankacılığı yoluyla vergi ödemeleri, kurum ödemeleri, online fatura ödemeleri, fatura talimatı işlemleri, SGK Ödemeleri, eğitim ödemeleri, Küçük ve Orta Büyüklükteki İşletmeler (KOBİ) ödemeleri gibi işlemleri yapabilirler. Ayrıca e-devlet İşlemleri, senet ödemeleri, bağış ödemeleri, doğrudan borçlandırma sistemi, portföy görüntüleme, menkul sermaye işlemleri, fon işlemleri, döviz işlemleri, altın işlemleri, repo işlemleri, bono/tahvil alış ve satışı, halka arz işlemleri, ticari destek kredi işlemleri, Toplu Konut İdaresi Başkanlığı (TOKİ) işlemleri, Esnaf ve Sanatkarlar Kredi Kefalet Kooperatifleri işlemleri ve şifre işlemleri gibi seçenekler bulunmaktadır.

3.6. İnternet Bankacılığının Özellikleri ve Kapsamı

3.6.1. İnternet Bankacılığının Avantajları ve Dezavantajları

Müşteriler ve bankalar internet bankacılığı kapsamında bazı avantajlara sahip oldukları gibi bazı dezavantajlara da sahip olmaktadırlar. Genel hatlarıyla internet bankacılığının sağladığı yararlar ve neden olduğu sorunlar şu şekilde ifade edilebilir. Sağladığı yararlar (Ayıgulıaılı, 2016);

- İstenilen noktada erişimi mümkün kılmaktadır. Bu açıdan internet bağlantısı olduğu sürece işlemlerin her yerden kontrol edilebilmesi mümkündür,
- Faaliyet ve yönetim açısından şube bankacılığıyla kıyaslandığında daha düşük maliyetlerle hizmet verilebilmesi mümkün olmaktadır. Bununla birlikte internet bankacılığıyla birlikte daha çok müşteriye ulaşılabilmesi mümkündür,
- Şube bankacılığında sıra bekleyerek zaman kaybı yaşanabilmektedir. Ancak internet bankacılığında sıra bekleyerek zaman kaybının yaşanması söz konusu olmamaktadır,
- İnternet bankacılığından genel olarak geliri yüksek müşteriler yararlandıkları için bankaların mevduatlarının artması söz konusu olmaktadır.

Ortaya çıkabilecek sorunlar ise şunlardır:

- İnternet bankacılığının siber saldırılara maruz kalması neticesinde müşteri hesaplarının çalınması söz konusu olabilmektedir.
- İnternet bankacılığıyla müşterilere iyi bir pazarlama faaliyetinin dijital pazarlamadaki eksiklikler nedeniyle yapılamayabilmektedir.
- İnternet bankacılığında işlemlerin yanlış yapılması halinde bu işlemlerin düzeltilebilmesi oldukça güç olmaktadır.
- Firmaların kendi internet siteleri kapsamında bankaların yapabildikleri işlemlerle ilgili verdikleri bilgiler ile bankaların internet sitelerinde yapabildikleri işlemlerle ilgili verdikleri bilgilerin farklı olması müşterilerin kafalarının karışmasına neden olmaktadır.

3.6.1.1. Banka İçin Avantajları ve Dezavantajları

Maliyetler, diğer alternatif dağıtım kanallarından çok daha düşüktür. Bir şube işleminin maliyeti 1,5 TL iken, internet bankacılığında bu maliyet 0,1 TL'ye düşürülebilir. İnternet bankacılığı sadece bilişim açısından bankanın ilerleme düzeyini göstermez, aynı

zamanda müşteriye sunduğu hizmet çeşitliliğini de arttırır ve bu da bankanın teknoloji açısından imajını arttırır. İnternet sitelerini çekici kılacak bankalar, ürünlerini çok daha ekonomik bir şekilde ilan edebilecek ve aynı zamanda şubeye gitmek zorunda kalmadan müşterinin emrinde daha sık yapılan işlemleri teşvik edeceklerdir (Yıldırım, 2006).

İnternet bankacılığı sistemi kurulma aşamasında sistemin sorunsuz işleyişi ve karşılaşılabilecek problemlere anlık olarak yanıt verebilmesi ve bu konuda destek verecek olan personelin istihdam edilebilmesi için belirli bir miktarda yatırım harcaması yapılması gerekmektedir. İnternet altyapısının ülkemizde yeterli olmaması, internet bankacılığı ve mobil bankacılık hizmetlerine erişimin yavaş olması, müşteriler açısından negatif etki yaratabilmektedir. Güvenlik kavramı internet bankacılığı kullanımında en önemli etkenlerden biridir. Güvenlik konusunda yaşanabilecek en küçük sorun bankaların müşteri sayısında ani bir düşüşe sebep olabilir. Bankalar açısından bir diğer dezavantajda internet bankacılığının müşteri kazanımında önemli bir role sahip olmasıdır. Çünkü günümüzde internet bankacılığının aktif olarak kullanılması müşterinin çok hızlı ve kolay bir şekilde bankasını değiştirebilme imkanının olmasını sağlamaktadır. Bu durum bankaların hedeflerine ulaşmada birtakım problemler yaşamalarına sebep olabilmektedir

3.6.1.2. Müşteri İçin Avantajlı ve Dezavantajları

En büyük avantajı belli bir yere bağlı kalınmaksızın internet iletişiminin olduğu her noktada 365 gün 24 saat ulaşımın mümkün olmasıdır. Her işlem her saatte gerçekleştirilememektedir. Ama bu işlemler için de ileri tarihli talimat verebilme imkânı vardır. Maliyetlerin düşük olması nedeniyle bankacılık işlemleri daha düşük bir ücretle yerine getirilebilir ve bunun neticesi olarak internet bankacılığı aracılığıyla açılan mevduat hesaplarına daha yüksek faiz almaları mümkündür. Şubelere ulaşmak için kullanılan vasıtaların yarattığı çevre kirliliğini ve şubelerde gerçekleştirilen işlemlerin çıktıları nedeniyle yaşanacak kağıt israfını önler. Kullanım kolaylığı sunmaktadır. Yapılan işlemlerin kayıtları bilgisayara liste halinde döküm yaptırılabilir. Bireylerin hesaplarını daha yakından takip edebilmesine imkân tanır ve hesaplarda yapılması muhtemel usulsüzlüklerin daha kısa süre içerisinde ortaya çıkarılmasını sağlar.

Banka ile müşteri arasında yaşanan ilişkinin zedelenmesine neden olur. Örneğin müşteri kendi ihtiyaçları doğrultusunda bir kredi çekme durumu olduğunda müşterinin internet bankacılığı tarafından tanınmaması bu ihtiyacının giderilmesini engellemektedir. Birtakım sorunlar internet bankacılığı aracılığı ile çözüme ulaştırılamayabilir. Bu durumda

müşteri şubeden işlem yapmak durumunda kalır. Şubeye giden müşterinin sorunlarının çözümünde daha çok uğraş yapılmakta veya müşterinin talebi doğrultusunda yatırım ve farklı konularda danışmanlık hizmeti de verilebilmektedir. İnternet bankacılığında bu durum söz konusu değildir (Koskosas, 2011).

3.7. İnternet Bankacılığı Tehditlerine Karşı Alınması Gereken Önlemler

İnternet bankacılığını kullanıcılar açısından cazip hale getirmenin en önemli unsuru güvendir. İnternet 21. YY'ın başlarından itibaren günlük hayatımızda oldukça önemli bir yer kaplamaya başlamıştır. Günlük bankacılık işlemlerimizin pek çoğunu internet aracılığı ile yaptığımız bir gerçektir. İnternet bankacılığı kullanan bireysel//kurumsal müşterilerin sayısı yadsınamaz olsa da bazı müşteriler hala bu yeni teknolojiye pek sıcak bakmamaktadır. Bunun temel nedeni de her ne kadar birçok önlem alınmış olsa da bazı güvenlik sorunlarının mevcut olmasıdır. İnternet bankacılığı işlemlerinin güvenli bir şekilde yapılabilmesi bazı için tedbirler vardır. Kullanıcılar işlemlerini yapmadan önce bir dizi güvenlik prosedürünü gerçekleştirmek zorundadır (Weiser, 2001).

Örneğin Türkiye İş Bankası'nın mobil uygulaması olan İşcep'i kullanmak isteyen müşterinin banka sisteminde kayıtlı olan telefon numarasına önce bir mobil onay kodu gönderilerek telefon numarasının doğruluğu kontrol edilir. Daha sonra doğruluğu teyit edilen bu telefon numarasına bir geçici şifre gönderilir. Müşteri 5 gün içerisinde bu geçici şifre ile İşcep'e giriş yaparak kendine kalıcı bir şifre belirler. Kalıcı şifresini belirleyen kullanıcıya İşcep kullanım şartları çerçevesinde, kalıcı şifresine ek bir güvenlik önlemi olarak iki seçenek sunulur. Ya İşcep'e her girdiğinde banka tarafından yeni bir mobil onay gönderilecek ya da kullanıcının kendi belirleyeceği bir "Cep Anahtar" şifresi ile sisteme giriş sağlanacaktır. Elektronik ortamda güvenliğin sağlanması açısından her ne kadar azami tedbirler alınsa da ticari casusluk ve siber saldırıların önüne pek geçilememiştir. Ancak bu güvenlik sorununu ortadan kaldırmak için pek çok yöntem geliştirilmiştir. Bunlardan bazıları;

3.7.1. Açık Anahtar Altyapısı

Verilerin aktarımında yaygın kullanılan bir yöntemdir. Bu sistemde asimetrik şifreleme yöntemiyle üretilen ve yönetilen anahtarlar temel alınır. Bu sistemde iki taraf mevcuttur. Bu taraflar asimetrik şifreler kullanarak bir oturum anahtarı belirler ve kendi aralarında oluşturulan simetrik şifreleme yöntemiyle iletişim sağlanır. Bu sistem asimetrik kriptografi sistemlerinin gerçekleşmesi ve açık, özel anahtarları yönetmek için kullanılır.

Bu sayede taraflar güvenilir bir şekilde işlemlerini gerçekleştirebilirler. Açık Anahtar Sistemi'nin temel bileşenleri (Weiser, 2001);

- Sertifika Otoritesi: Sistemin en yüksek ve diğer kullanıcılarının tamamının güven duyduğu bir mertebedir. Bu otorite diğer sertifika sahiplerinin kimlik ve açık anahtar eşleşmelerinden sorumludur. Sayısal sertifikalar üreterek bilgilerin güncelliğini korur ve iptal edilmesi gereken sertifikalar ile ilgilenir.
- Kayıt Makamı: Sertifika talep edenleri kimlik denetimine tabi tutarak sertifika otoritesine yönlendirir.
- Merkezi Sertifika Deposu: Sertifika ve iptal listeleri ile ilgilenen bölümdür.
- Anahtar Çiftleri: Özel ve Genel Anahtarlardır.
- Sayısal Sertifikalar: Sertifika otoritesi tarafından onaylanmış güvenlik araçlarıdır. Kullanıcılar sisteme giriş yapmaya çalışanların kendileri olduğunu ispat etmek için açık anahtarlarını Sertifika Otoritesine onaylattırır. Bu sayede Açık Anahtar Sistemi ögeleri kullanıcının kimliğini teyit etmiş olur. Sayısal sertifikaların kullanıldığı bazı uygulamaları şu şekilde sıralayabiliriz:
    - Elektronik posta iletişimi,
    - Kablosuz bağlantılarda güvenlik,
    - VPN,
    - IPSec ile güvenilir veri iletişimi,
    - Web tarayıcılarında bulunan sertifika ile kimlik doğrulama işlemi,
    - EFS ile veri şifrelemesi,
    - Disk şifreleme,
    - Akıllı kart ile kimlik doğrulama ve oturum açma,
    - SSL ve TLS ile güvenli veri iletişimi,
    - LDAP,
    - Dijital imza ile belgelerin imzalanması,
    - Anlık mesajlaşma. Sertifikanın geçerli sayılabilmesi için 3 önemli nokta vardır.
    - Sistem saati, sertifikanın geçerliğinin başladığı ve sona erdiği tarihler arasında olmalı,
    - İptal edilmemiş durumda olmalı,
    - Makinede yüklü güvenli köklerden oluşmalı.

Alınacak sertifikalar; tarafsızlığı ve güvenilirliği doğrulanmış Sertifika Otoriteleri'nden temin edilmeli, en az 2048 bit anahtar çiftine sahip olmalı, sertifikalar sigorta koruması altında olmalı.

3.7.2. Elektronik İmza

Elektronik ortamdaki bir belgeye eklenerek imzalayanın kim olduğunu bilmeye yarayan bir sistemdir. 5070 Sayılı Kanun'a göre e-imza, ıslak imza hükmündedir. Eimza sertifikası, bu sertifikayı dağıtmaya yetkili kuruluşlar tarafından temin edilir. Bu kuruluşlar;

- Elektronik Bilgi Güvenliği A.Ş. (E-Güven),
- TUBİTAK-UEKAE (Kamu. Sertifikasyon Merkezi),
- TürkTrust Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.,
- EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-Tugra),
- Emniyet Genel Müdürlüğü Sertifikasyon Merkezi (EGMSM),
- E-İmza Bilgi Güvenliği Hizmetleri A.Ş. (e-İmzaTR)

3.7.3. Mobil İmza

Cep telefonu ve GSM SIM kart kullanarak 507 sayılı Elektronik İmza Kanunu ile ilgili mevzuata uygun olarak ıslak imza eşdeğerinde işlemlerin güvenli bir şekilde yapılmasını sağlar.

3.7.4. Güvenlik Duvarı

Güvenlik duvarı ağı ve internet ağı arasında tampon görevi koyan bir donanım ya da yazılım ögesidir. Sistemi kullanma yetkisi olmayan kişilerin ağa giriş yapmasını ve bilgilere ulaşmasını engelleyerek kötü niyetli kişileri sistemden uzaklaştırmaktadır. Buna ek olarak kullanıcıların ziyaret ettiği sitelerin güvenliğinden emin olmazsa işlemlerini kısıtlayabilmektedir. Bankalar sistemleri koruma altına almak adına birçok yatırım yapmakta ve güvenlik prosedürlerini artırmaktadır. İnternet bankacılığının tam anlamıyla güvenli sayılabilmesi amacıyla bankalar bağlantılarının ne gibi durumlarda farklı sistemlerle etkileşim içine girip giremeyeceklerini düzenlerler. Bu düzenlemeyi yaparken kullanılan etmenlerden biri de güvenlik duvarlarıdır. Güvenlik duvarları sadece sistem güvenliğine tahsis edilmişlerdir. Güvenlik duvarları ana sistemle, dış sistemler arasında yer alır. Ana sisteme, dışarıdan gelen her bir bağlanma isteğini kontrol ederek tehlikeli bağlantıları engeller. Banka içi bağlanma istekleri de en az dışarıdan gelen istekler kadar denetime tabi tutulmaktadır.

3.7.5. Güvenli Yuva Katmanı

1994 yılında Netscape Communications Corporation şirketi geliştirmiştir. Sunucu ile sisteme giriş yapmak isteyen kullanıcı arasında kurulacak iletişimin şifreli bir şekilde yapılmasını sağlayan, bu sayede bağlantının güvenli bir biçimde sağlanmasına yarayan protokoldür.

3.7.6. 3D Güvenlik Kodu Sistemi

Visa ve MasterCard tarafından tasarlanan bu sistemin amacı internet alışverişlerini güvenli bir hale getirmektir. Visa tarafından sunulan 3D Güvenlik sistemi Verified by Visa olarak adlandırılırken, MasterCard 'ın sunduğu uygulamaya Secure Code denir

3.7.7. İki Faktörlü Kimlik Doğrulama Sistemleri

2000'li yılların başında kullanılmaya başlayan bu sistem bugün pek çok banka tarafından kullanılmaktadır. Bankalar internet bankacılığı hizmeti sunarken kullanıcı bilgi ve şifrelerini kontrol ederler. Kullanıcılar internet bankacılığı hizmetinden yararlanmak isterken bu bilgiler ile sisteme giriş yaptığında, kötü amaçlı bilgisayar korsanları kullanıcı bilgilerini ele geçirebilmektedirler. Bu istenmeyen durumu önlemek için tek kullanımlık şifreler kullanılmaktadır. Bu tek kullanımlık şifreler ya sadece bu şifreyi oluşturmak amacıyla tasarlanan minik elektronik aletler veya telefonlarda bulunan uygulamalar aracılığıyla verilmektedir. Zaman tabanlı, soru-cevap veya işlem imzası gibi ek özelliklerinin olması güvenlik derecelerini artırmaktadır (Yücel, 2012).

3.7.8. Titreşimli İşlem Doğrulama Sistemi

İnternet bankacılığı kullanıcıları işlemlerini tamamlamak aşamasında çipli kart okuyucular üzerindeki tuşlar aracılığıyla paranın gönderileceği hesap numarası ve işlemin meblağsını tuşlarlar. Okuyucular da girilen bu bilgileri belirli bir algoritma şeması aracılığıyla o anki işleme ait bir koda dönüştürür. Bu kod kullanıcıya iletilir ve kullanıcı bu koda onay verir. Ancak bu kodun her internet alışverişinde yenilenmesi ve kullanıcıların bu işlemleri baştan tekrar etmesi gerektiğinden kullanıcılar bunu kullanışsız ve zahmetli bulunduğu için tercih edilmemektedir. Kullanıcıları bu zahmetten kurtarmak amacıyla optik kart okuyucu sistemi geliştirilmiştir. Bu sistemde kullanıcılara paranın gönderileceği hesabı tuşlamak ve bilgisayar ekranına gelen titreyen şekil içeren kodu telefonlarının kameralarına okutmak kalmaktadır.

3.7.9. Biyomotorik Tabanlı Kimlik Doğrulama Sistemi

Kişiye has fizyolojik özellikler temel alınarak -parmak izi, DNA, yüz, iris, ses, el içi, avuç içi damar izi- oluşturulan bir güvenlik sistemidir. Bu sistem çok maliyetli ve kötü kişiler tarafından ele geçirilmesi halinde dönüşü çok zordur. Ancak kişinin fizyolojik özellikleri dışında ek bir güvenlik önlemi gerektirmemesi bu sistemi oldukça kullanışlı kılmaktadır (Şamlı ve Yüksel, 2009).

3.7.10. İşletim Sistemi Güvenlik Güncellemeleri

Güvenlik sistemlerini üreten firmalar zaman zaman güncellemeler yaparak güvenlik sistemlerini geliştirip, güçlendirirler (Dayıoğlu, 2017).

3.7.11. Anti-Virüsler

Bilgisayar virüsleri, bilgisayarların içindeki verilere ya zarar vererek kullanılamaz duruma getirir ya da tamamen silinmelerine neden olur. Temel virüsler sıradan bilgisayar kullanıcılarını etkilerden, komplike virüsler e-posta paylaşma uygulamaları gibi başka yazılım sistemlerini denetleyerek çoğalabilirler. Bazı virüsler de yararlanmış gibi gözükürken aslında bilgisayara ve işletim sistemlerine zarar verirler. Bunların en bilineni Truva Atı'dır. Antivirüs programları bu gibi zararlı yazılımların bilgisayara girmesini engeller (Barışık ve Temel, 2007).

3.7.12. AntiSpyware

Adware yazılım programcılarının masraflarını telafi edebilmek amacı ile programlarına reklam eklemelidir. Bu reklam uzantıları kullanıcıların en çok hangi siteyi ziyaret ettiğini takip eder. Ayrıca sisteme ve bilgisayara zarar verebilecek pek çok programcı da sisteme girebilir. İşte bu işlemin adı Spyware'dir (Akça, 2005).

3.7.13. Sanal Klavye

Kullanıcıların bilgisayarlarının fiziksel klavyelerini kullanmadan, ekran üzerinde bulunan tuşları tıklayarak şifrelerini girmelerini sağlayan bir sistemdir. Ancak kullanıcıların bilgilerini çalmaya çalışan hackerler keylogg adı verilen bir casus programla klavye hareketleri kaydederek kişilerin bilgilerini ele geçirirler. Bu keylogg programlarını etkisiz hale getirmek için sistem sunucuları "Kaspersky" adı verilen koruyucu programları geliştirmişlerdir (Öztürk, 2006). İnternet bankacılığı kullanıcılarının dikkat etmesi gereken güvenlik önlemlerini sıralamak gerekirse;

- İnternet Şubesi güvenliği ile ilgili sorular, tereddüt edilen konular ve olağandışı durumlar için vakit kaybetmeden bankaların çağrı merkezileri aranmalı,

- Bankalar ve Türkiye Bankalar Birliği tarafından yayımlanan bilgilendirme ve uyarılar düzenli aralıklarla takip edilmeli,
- Kullanıcı kodu ve şifre ile internet bankacılığına giriş yaptıktan sonra ilk ekranda giriş yapılan son işlem tarihi ve saatini kontrol edilmeli,
- Kimliğinizin taranmış görüntüsünü bilgisayarda saklanmamalı,
- İnternet bankacılığı şifresi herhangi bir yere yazılmamalı veya bilgisayara/telefona kaydedilmemeli,
- İnternet kafeler veya ortak kullanıma açık bilgisayarlarda internet bankacılığı işlemi yapılmamalı, internet bankacılığı oturumunuzu sonlandırmadan bilgisayar terk edilmemeli,
- Güvenli olmayan internet sitelerinden dosya - program indirilmemeli,
- Bankalar kişisel bilgileri müşterilerden e-posta yoluyla talep etmemektedir. Kullanıcı bilgileri talep edilen e-postalara kesinlikle cevap verilmemeli, derhal banka ile iletişime geçilmeli,
- Bilinmeyen göndericilerden gelen e-postalar açılmamalı ve beraberindeki ekler indirilmemelidir,
- İnternet bankacılığı ekranında şüpheli bir ekran görüntüsü ile karşılaşıldığında giriş yapılmamalı ve bankalar ile iletişime geçilmeli,
- Bilgisayarlarda sahte yazılımlar kullanılmamalı ve güncellemeler takip edilmeli,
- Bilgisayarlarda "anti-virüs" ve "güvenlik duvarı (firewall)" programlarının güncel versiyonları kullanılmalı,
- İşlem yapılmak istenilen sayfaların bankalara ait olduğundan emin olunmalı, internet adresi tarayıcı ekranına şahsen yazılmalı,
- İnternet bankacılığı işlemi bittiğinde her zaman güvenli çıkış butonunu kullanılmalıdır.

Bankaların uyması gereken güvenlik önlemlerini sıralamak gerekirse arlı yazılımların bilgisayara girmesini engeller (Barışık ve Temel, 2007);

- Bilgisayarların tamamında güncel virüs programları kullanılmalı,
- Tüm network bağlantılarının güvelikleri sağlanmış olması,
- E-postalar ve e-posta eklerinde gelen dosyalar için virüs taraması yapılmalı,
- Kişisel bilgisayarların modemleri kayıt altına alınmalı, Şifreler tüm çalışanlarla paylaşılmamalı ve ritmik aralıklarla güncellenmeli,

- Bilgisayar korsanlarına karşı, internet bankacılığı sistemi belirli aralıklarla testler yapılmalıdır.

3.8. İnternet Bankacılığında Blok Zincir Kullanımı

Blok zincir teknolojisinden önce internette küresel geçerliliği bulunan dijital para birimi meydana getirilmesine ilişkin pek çok girişim gerçekleştirilmiştir. Fakat bu girişimler "çift harcama" sorunu nedeniyle hedefine erişememiş ve başarısız olmuştur. Çift harcama sorunu dijital para birimlerine özgü bir problem olmakla beraber aynı dijital paranın iki farklı alım satım işleminde ele alınarak satıcılardan birinin dolandırılmasıdır. Dijital paralar, internet alanında saklı tutulabilen diğer bütün veriler gibi bir bit dizisidir ve kopyalanmaları göreceli olarak kolaydır. Mesela, bir pdf belgesi başka bir bireye gönderildiğinde, alıcıya belgenin dijital bir kopyası iletilir ve belgenin orijinali gönderen bireyde kalır. Bu belgenin farklı bir bireye daha iletilmesi, bireyin ona ulaşmasına engel olmayacaktır. Bu durum kullanıcılara dijital bilgileri çoğaltıp, başka bireylerle paylaşma olanağı tanısa da dijital para birimleri için kritik bir güvenlik açığına yol açacak niteliktedir (Pisa ve Juden, 2017:5-7).

Blok zincir teknolojisi bu güvenlik açıklarını ve özellikle dijital paralarda bulunan çift harcama sorununu gidermek için öne sürülen elektronik ödeme sistemidir. Özetle blok zincir; güvenlik açıklarına karşı korumalı ve kolay bir şekilde ulaşılabilen bir ağda şifrelenen verileri yöneten dağınık veri tabanıdır. Blok zincir teknolojisini günümüz ağlarından farklı kılan eşler arası ağ, dağıtılmış defter, mutabakat mekanizması ve kriptografi teknolojileridir (Pisa and Juden, 2017: 5-7):

Eşler Arası Ağ: Blok zincir teknolojisinde ağda yer alan her katılımcının kendine özgü senkronize edilmiş bir kopyası vardır. Böylece katılımcılar ağda meydana gelen faaliyetleri görebilir ve bunlara onay verebilir. Bu durum ağda yer alan merkezi otoriteyi yok ederek katılımcıları doğrudan birbirine bağlar.

Dağıtılmış Defter: Blok zincir ağında yer alan bütün katılımcıların meydana getirdiği faaliyetlerin kaydedildiği dijital hesap defterleridir. Günümüz bilgi işlem teknolojilerinin geneli tek bir merkezi ağda faaliyet göstermektedir. Merkezi ağlarda dijital defterlere kaydedilen veriler sunucularda bir araya getirilir ve buradan istemcilere dağıtılır. Eşler arası ağdaysa katılımcılar gerek sunucu gerek istemci konumundadır. Meydana gelen bütün faaliyetler katılımcılara ilişkin senkronize edilmiş defterlere eş zamanlı şekilde işlendiğinden merkezi sunucu kaynaklı güvenlik açıkları ortadan kaldırılmaktadır.

Mutabakat Mekanizması: Eşler arası ağda yer alan bir katılımcı bireysel dijital hesap defterine veri girişi yapmayı düşündüğünde, bu işlem bilinen algoritmalar ele alınarak kodlanır ve ağda yer alan bütün kullanıcılara bilgi verilir. İşlem, kullanıcılar arasında mutabakata varılıp doğrulandığında veri kalıcı kayıtlara dahil edilir. Ağda yer alan bütün katılımcılar aynı kayıtlı verilerle çalıştığından kaydı gerçekleştirilen işleme itiraz edilemez ve değiştirilemez.

Kriptografi: İnternette meydana getirilen kullanıcı kimliği ya da belgelerin bütünlük doğrulamaları gibi faaliyetlerde dijital imza ele alınmaktadır. Dijital imzalar kullanıcıların özel anahtarlarıyla meydana getirilir ve alıcılar kullanıcılara ilişkin genel anahtarları ele alarak bu imzaları kontrol edebilirler. Blok zincir teknolojisinde bir işlemin imzasının doğrulanmasının ardından özel ve genel anahtarlar kriptografik şekilde "hash" olarak adlandırılan şifreleme tekniğiyle matematiksel algoritmayla bağlanarak benzersiz bir dijital imza meydana getirilir. Sonrasında bu işlemler blok haline getirilir. Meydana getirilen her blok ağa daha önce eklenmiş bloklara ilişkin kayıtları bozmadan zincire dahil edilir ve ağda yer alan kullanıcıların dijital hesap defterlerine kaydedilir.

Blok zincir ağında meydana getirilen her bir veri bloğu kendinden önceki bloğun hash'ine bağlanır ve ilk bloktan son bloğa dek uzanan bir zincir meydana getirilir. Zincire kaydedilen veri harici müdahaleyle değiştirildiğinde, verinin kayıtlı olduğu blok, zincirde yer alan bütün bloklarla ilişkili olması nedeniyle yapılmaya uğraşılan müdahale her birinde değişikliği tetikleyecektir (Pisa and Juden, 2017:9). Bu durum ağda meydana getirilmek için uğraşılan faaliyetin belirlenmesini kolay hale getirecektir. Bunun yanı sıra blok zincirine müdahaleyle yeni blok ilave edilmek istenilirse bütün bloklara ilişkin düğümler çözümlenerek ağın gerisinde bırakılmalıdır. Bu da Blok zincir ağına dışarıdan meydana getirilebilecek muhtemel müdahaleleri oldukça zorlu ve maliyetli bir duruma ulaştırdığından dijital paraların en büyük problemi olan çift harcama sorununu yok edecektir (Krause ve diğer., 2016:8).

İnternetin kişiler arasında yaygınlaşması iktisadi uygulamaların internet tabanlı platformlardan devam ettirilmesinin önünü açmıştır. Bankacılıktan borsa faaliyetlerine, resmi işlemlerden alışverişe dek birçok işlem internetten kolay bir şekilde gerçekleştirilebilmektedir. Fakat bu işlemlerin merkezi sunucular aracılığıyla sürdürülmesi ve iktisadi faaliyetlerde ele alınan sitelerin güvenlik açıklarının bulunması kişilerin ya da kurumların verilerinin çalınmasına yol açmaktadır.

Özellikle internet bankacılığı faaliyetlerinde bu durumla sık sık karşılaşılmaktadır. Dijital paraların meydana gelmesiyle başlayan süreçte blok zincir teknolojisinin bilinirliliğinin çoğalması güncel finans sisteminin eksik taraflarını daha da belirgin hale getirerek tartışmaya açmıştır. Zira Blok Zincirin getirdiği DDT ve akıllı sözleşmeler gibi önemli teknolojiler, modern iktisadi sisteminin temelini meydana getiren bankacılık sektörünün sürdürdüğü faaliyetlerdeki maliyet, işlem süresi, işlem hatası ya da verilerin/paranın çalınması gibi problemlere çözüm sağlayabilecek kapasiteye sahiptir.

Blok zincir hakkındaki akademik çalışmaların yaklaşık %80'i Bitcoin odaklıdır. Araştırmaların %20'den daha az kısmıysa akıllı kontratlar dahil olmak üzere blok zincir uygulamaları üzerinde durmuşlardır. Buna ilaveten, verimlilik kapasitesi ve gecikme süresi gibi blok zincirin ölçeklenebilirlik hakkındaki sorunlarını araştırmacılar dikkate almamıştır. Blok zincirin, büyük ölçekte ve bilhassa bankacılıkta ele alınabilmesi için, kendisini tam anlamıyla ispatlamamış olmasına karşın gerek akademi gerekse de özel Ar-Ge merkezleri ölçeklenebilirliği ve sunabileceği çözümler bakımından yoğun araştırmalar gerçekleştirmektedir. Bu araştırmalar, ileri kriptografik, dağıtık sistemleri ve oyun kuramını araç olarak ele almaktadır.

Blok zincir teknolojisinde her bir katılımcı, başlangıçtan beri bütün kayıtların bir kopyasını tutar. Bu kayıtların değiştirilmesi özetlerin değişmesine yol açacağından ötürü kayıtlar değiştirildiğinde çoğunluk bunu fark edebilir. Bundan dolayı güvenilir ortamda merkezi bir veri tabanı gereksinimi kalmaz. Herkesin doğrulama yapabildiği dağıtık bir veri tabanı sistemiyle kimseye güvenmeye gerek kalmadan doğru bilginin tutulduğu ispatlanabilir.

4. KURAMSAL ÇERÇEVE – TEKNOLOJİ KABUL MODELİ

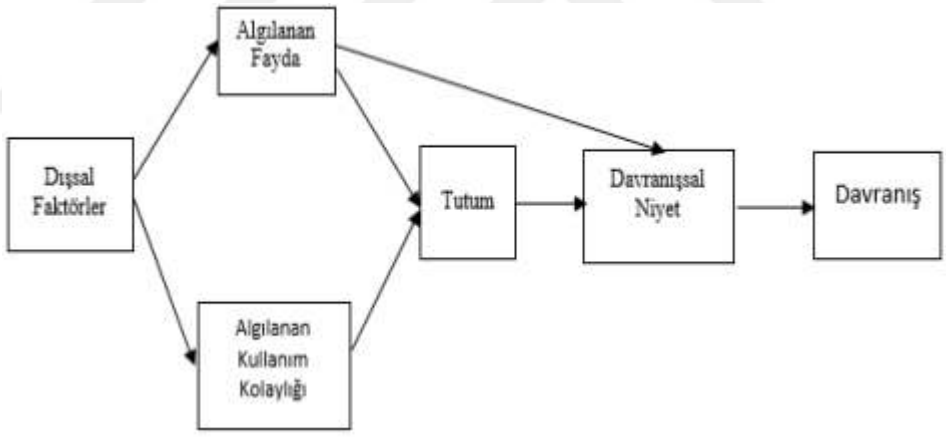
Literatürde, belirli bir teknolojiye karşı kullanıcıların davranışlarını inceleyen birçok model geliştirilmiştir. Bu bölümde bu modeller açıklanmış ve blok zincir teknolojisinin kabulünü inceleyen çalışmalar verilmiştir.

4.1. Teknoloji Kabul Modeli-Technology Acceptance Model (TKM)

Teknolojinin değişmesi ve gelişmesi ile ortaya çıkan yenilikler, insanlar tarafından tam olarak algılanamadığında belirsizliklere neden olmakta ve insanların yenilikleri benimsemesi zaman almaktadır. Bu noktada teknoloji kabul modeli de yenilikleri tam olarak algılayamamış ya da benimseyememiş insanların teknolojiyi kabul veya reddetme durumlarını yani adaptasyonlarını açıklamaya çalışmaktadır (Davis, vd., 1989).

Teknoloji kabul modeli bilgi teknolojilerinin, iş ortamında kabulünü tahmin etmek ve açıklamak için geliştirilmiş olmasına rağmen diğer teknolojik gelişmelerin benimsenmesinin, açıklanmasında da kullanılmaktadır. Daha pek çok teknolojik ürün, hizmet, yaratıcı yenilik için modelin uygulanması, teknoloji kabul modelini iş ortamının dışında günlük hayatta da kullanılır duruma getirmiştir. Sebepli Davranışlar Teorisini temel alan bu model (1989) yılında Davis tarafından geliştirilmiş ve ölçeklendirilmiştir (Zeren, 2018: 171;Davis, vd., 1989).

TKM'nin diğer modellere göre daha çok uygulanmasının nedeni açık ve anlaşılır olmasıdır. Bu model, daha önce kullanılan modellerin teorik alt yapılarını kullanım kolaylığı, algılanan fayda, kullanımla ilgili tavır, kullanım niyeti ve gerçek kullanım arasındaki ilişkileri açıklamaya çalışmaktadır. Genel anlamda TKM bilgi sistemleri teorisi olarak nitelendirilmekte ve toplumun teknolojiye bakış açısını ve nasıl kabul ettiğini teorik olarak modellemeye çalışmaktadır. TKM dört temel unsurdan oluşmakta ve bu unsurlara dayanarak ölçülmektedir. Bu unsurlar; algılanan fayda, algılanan kullanım kolaylığı, tutum ve davranışa yönelik niyettir (Atik, 2015: 44; Davis, vd., 1989).



Şekil 3 Teknoloji Kabul Modeli (TKM)

Kaynak: Davis, vd., 1989

Algılanan Fayda: TKM' de yer alan ilk değişkendir, kişilerin iş performanslarının teknoloji kullanılması ile birlikte artacağına inanma derecesi olarak tanımlanır. Bu tanıma göre kişilerin teknoloji kullanım-performans ilişkisinin pozitif olduğu bir sistemde algılanan fayda yüksek olmaktadır. Aynı zamanda algılanan fayda kullanım kolaylığı ile birlikte tutumu etkilemektedir, algılanan fayda değişkeni davranışsal niyet üzerinde de doğrudan etkiye sahiptir ve davranışsal niyetin güçlü bir belirleyicisidir. Bu doğrultuda da davranışsal niyet üzerindeki, etkisi ile insanların iş performanslarını arttıracağına

inandıkları davranışlara yönelik niyetler oluşturduğu fikrine dayanmaktadır (Seyhan, 2019; Davis, vd., 1989).

Algılanan Kullanım Kolaylığı: Algılanan Kullanım Kolaylığı da, Algılanan Fayda unsuru gibi TKM'nin temel unsurlarındandır. Algılanan kullanım kolaylığı bireyin, bir sistemi ya da teknolojiyi kullanırken zorluk yaşamamasını ifade eder. TKM'ye göre algılanan fayda ve algılanan kullanım kolaylığı, bireyin yeni teknolojiye karşı tavrını etkilemektedir. Algılanan kullanım kolaylığının artması, kişinin performansının dolayısıyla da algılanan faydanın artmasında etkilidir ve birey ne kadar kolay sisteme erişebilir ve kullanabilirse o derece sistemi, teknolojiyi kabul ettiği gözlenmektedir (Kılıç, 2015: 67; Davis, vd., 1989).

Tutum: Tutum bireyin bir olay ya da nesneye karşı, söz konusu davranışı gerçekleştirme konusunda olumlu ya da olumsuz değerlendirmede ve tepkide bulunması eğilimidir. Tutum söz konusu davranışa yönelik niyet ve gerçekleşen söz konusu davranışı belirleyen önemli bir unsurdur, bireyin davranışı gerçekleştirmenin olumlu ya da olumsuz olduğu konusundaki kararını aynı zamanda bireyin davranışı gerçekleştirmeye niyetinin olup olmadığına karşı genel bir kanı oluşturmaktadır çünkü tutum davranışı yerine getirme niyetini devamında da davranışın kendisini etkilemektedir (Eroğlu, 2019: 34). Tutum doğuştan var olan dürtü değil, sonradan öğrenilen bir dürtüdür ve bu dürtü deneyimler, aile, inanç, çevre, sosyal ve psikolojik dinamikler gibi faktörlerden etkilenerek zaman içinde değişebilmekte ve bireyin nesnelere, kişilere veya olaylara karşı tutumunu etkilemektedir (Çakar, 2018: 71; Davis, vd., 1989).

Tutumun üç boyutu bulunmaktadır. Bu boyutlar;

Bilişsel Boyut: Bireyin nesne hakkında sahip olduğu bilgi, düşünce ve inançları ifade etmektedir. Bilişsel boyut tutumun rasyonel ifadesidir, bilişsel boyut için gerekli olan, bilgiye sahip olmaktır. Bilginin doğruluğu ya da yanlışlığı ile ilgilenmez.

Duygusal Boyut: Tutumun duygularla olan ilişkisini ve bireyin nesnelere ya da olaylara karşı duygularını ifade eder, Bilişsel boyuta göre daha basit yapıdadır (Pazvant, 2017: 31).

Davranışsal Boyut: Bireyin söz konusu olay ya da nesneye karşı olumlu veya olumsuz tepki gösterme durumunu ifade eder. Davranışsal boyut, duygusal ve bilişsel boyuta uyumluluk gösterir, duygusal ve bilişsel bileşenin bir sonucu olarak tutumun davranış haline gelmesinin ifadesidir (Bayraktar, 2019: 62).

Bu üç boyut birbirinden ayrı düşünülemez, tutumu etkiledikleri gibi birbirlerini de etkilemektedirler. Bu nedenle söz konusu davranışa karşı tutum oluşturulacak ise süreç birlikte takip edilmelidir. Aynı zamanda tutum, algılanan fayda ve algılanan kullanım kolaylığı ile belirlenmektedir, tutum davranışın öncüsüdür ve davranışa yönelik tutum TKM'nin açıklayıcısıdır.

Davranışsal Niyet: Bireyin söz konusu davranışı gerçekleştirmesine yönelik çabasının ve istemlerinin ölçüsüdür. TKM'ne göre davranışsal niyet, davranıştan hemen önceki aşamadır ve davranışı direkt olarak etkilemektedir. Aynı zaman da teknoloji kabul modeline göre; teknolojilerin bireyler tarafından sahiplenilerek kullanılmasının ilk belirleyici unsuru davranışsal niyet olmasıyla birlikte, bu unsurun belirleyicisi de teknoloji kullanmaya yönelik olumlu veya olumsuz fikirlerini ortaya koyan tutumdur. Davranışsal niyet, tutum ve gerçekleşen davranış arasında dolaylı bir ilişki kurmaktadır fakat algılanan fayda ve tutumdan direkt olarak etkilenmektedir (Bayraktar, 2019: 62; Davis, vd., 1989).

TKM'nin teknoloji kullanımının olumlu ve olumsuz yönlerini başarılı bir şekilde açıkladığı görülmüş ve bu nedenle günümüze kadar pek çok araştırma ve çalışma içerisinde yer almıştır ve TKM birbirinden farklı bilgi teknolojileri üzerinde uygulanmıştır. İnternet, intranet, e- ticaret için kullanılan akıllı kartlar, kablosuz teknoloji, mobil oyunlar, kısa mesaj teknolojisi, e-öğrenme ve daha birçok çalışmada yer almıştır (Erdem, 2011: 29). Teknoloji kabul modeli ile alakalı yapılan tüm çalışmalarda, kullanıcıların farklı teknolojileri nasıl ve neden kabul ettikleri ya da reddettikleri ortaya çıkarılmaya çalışılmıştır.

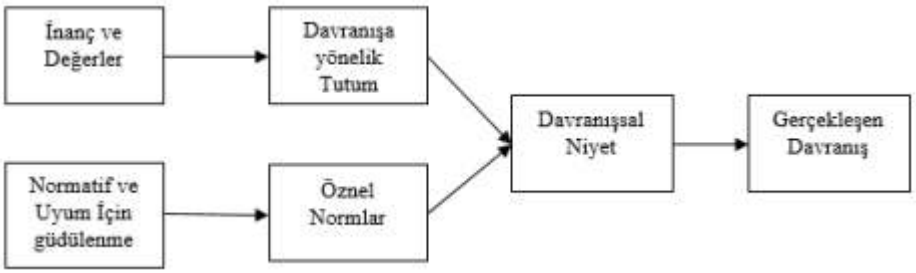
Fakat TKM'yi insanların teknolojiyi kabul veya ret durumunu açıklayan ve geçerliliği günümüzde de devam eden bir model olsa da bu modele de getirilen bir takım eleştiriler vardır bu eleştiriler; TKM'nin kullanıcılara yönelik olması, örgütsel kullanımında etkili olmaması, TKM'nin algılanan fayda ve kullanım kolaylığını etkileyen sistem özelliklerine yeterince değinmemesi, sosyal etmenlere yer vermemesi gibi nedenlerle eleştirilmektedir ve bu eleştirilerin sonucunda TKM'nin diğer teknoloji kabul modelleri ile birleştirilmesi ve genişletilmesi istenmektedir. Bu eksikliklerin giderilmesi içinde TKM 2 ve 3 olarak revize edilmiş eklenmesi gereken değişiklikler eklenmiştir.

4.2. Sebepli Davranışlar Teorisi (Theory Of Reasoned Action-SDT)

Sebepli Davranışlar Teorisi 1975 yılında Ajzen ve Fishbein tarafından ele alınmıştır. (Fishbein ve Ajzen, 1975). Sebepli Davranışlar Teorisi nin genel amacı, insan

davranışlarını önceden tahmin edebilmek ve anlamaktır. Bu teori temelinde sosyal psikolojiye dayanarak, insan iradesine bağlı olan davranışlara odaklanır. Aynı zamanda bu teorinin gelişimi teknoloji kabul modelini ortaya çıkarmıştır (Alipour, 2017: 25). Fishbein ve Ajzen'e göre insan davranışı üzerine çalışmalar yapılan bu teoride, insan davranışının en temel belirleyicisi kişilerin davranışı gerçekleştirmeye yönelik niyetidir, davranışsal niyet üzerinde ise tutum ve öznel normlar gibi faktörler etkilidir, fakat sebepli davranışlar teorisi, genel bir model olması sebebiyle davranışa ait inançları açıklamamaktadır (Fishbein. ve Ajzen, 1975).

Bu teoride "niyetin" davranıştan önce geldiği ve niyetin tutum ve öznel normlardan etkilendiği belirtilmektedir, yani kişinin performansını belirleyen davranış, bireyin davranışsal niyetine bağlıdır. "Davranışsal niyeti" ise bireyin tutumu ve öznel norm belirlemektedir. İnanç ve değerlerde "davranışa yönelik tutumu" belirlerken, uyum için güdülenme ve normatif inançlarda "öznel normu" etkilemektedir. "Davranışsal niyet" te gerçekleşen davranışı etkilemektedir (Çelik, 2018: 37; Davis, vd., 1989).



Şekil 4 Sebepli Davranışlar Teorisi

Kaynak: (Fishbein. ve Ajzen, 1975).

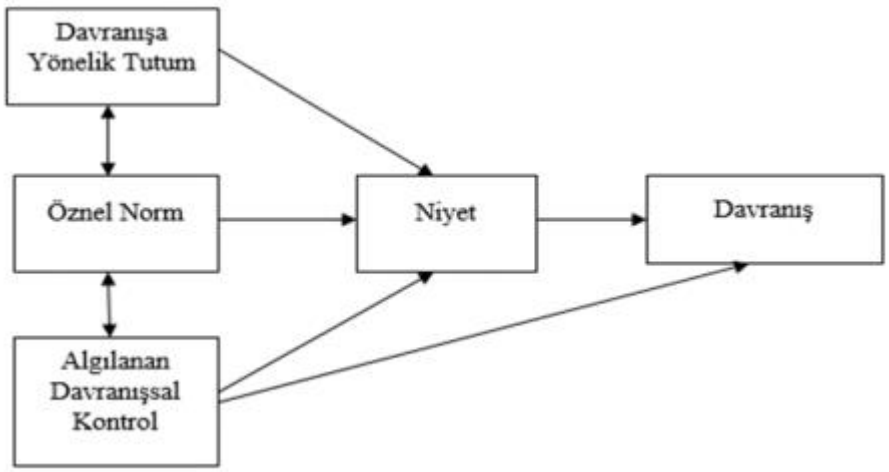
Sebepli davranışlar teorisinde yer alan, inanç ve değerler bu teoriyi zayıflatmaktadır ve bu teori bireyin bilgi ve beceri sahibi olmayı gerektiren ya da bireyin işbirliği içinde olmasını gerektiren davranışlarını açıklamada yetersiz kalmaktadır ve sebepli davranışlar teorisine göre insanın kontrolündeki davranışlar açıklanabilirken, bu davranışların ortaya çıkma koşulları her zaman buna uygun olmayabilir. Bu nedenle sebepli davranışlar teorisindeki zaafı kaldırabilmek için "algılanan davranış kontrolü" Ajzen ve Madden (1986) tarafından yeniden revize edilen planlı davranış teorisi modeline yerleştirilmiştir (Erten, 2002: 219).

Sebepli davranışlar teorisine yönelik yapılan araştırmalarda; düşünülmüş eylem teorisi, sebepli eylem teorisi, mantıklı eylem teorisi, nedenli eylem teorisi, akılcı davranış teorisi gibi, anlam olarak birbirine yakın fakat birbirinden farklı terimlerle kullanılmaktadır.

4.3. Planlanmış Davranış Teorisi (Theory Of Planned Behavior – PDT)

İlk olarak 1975 yılında Fishbein ve Ajzen tarafından ortaya atılan Planlanmış Davranış Teorisi, 1991 yılında Ajzen tarafından Sebepli Davranışlar Teorisi temel alınarak geliştirilmiş ve düzenlenmiştir (Fishbein. ve Ajzen, 1975). Bu düzenleme ile algılanan davranışsal kontrol öğesi sebepli davranışlar teorisine eklenerek bireylerin tamamen kontrol edemedikleri davranış durumlarını da kapsayacak şekilde ele alınmış ve planlanmış davranış teorisi oluşturulmuştur, bu düzenleme sonucunda ise iki teori arasında ki en önemli fark algılanan davranış kontrolü öğesinin eklenmesi olmuştur (Fishbein. ve Ajzen, 1975).

Planlanmış davranış teorisi kişilerin davranışlarını gerçekleştirebilmelerinin kolaylığını ya da zorluğunu ifade eden algıdır, amacı bireylerin söz konusu davranışlarını belirli bir çerçevede tahmin etmek ve açıklamaktır. Planlı davranış teorisi de sebepli davranışlar teorisi gibi kişilerin bir davranışı gerçekleştirmelerindeki birincil faktörün "niyet" olduğunu savunmakta ve kişilerin niyetlerini etkileyen üç temel faktör olduğundan bahsetmektedir. Bu faktörler; "davranışa yönelik tutum", "öznel norm" ve "davranışsal kontrol" dür (Ajzen, 1991).



Şekil 5 Planlanmış Davranış Teorisi Modeli

Kaynak: Ajzen, 1991

Davranışa Yönelik Tutum: Bireyin, gerçekleştireceği davranış konusunda olumlu ya da olumsuz değerlendirmesini ifade eden, öznel norm ve algılanan davranışsal kontroldür.

Öznel Norm: Bireyin söz konusu davranışı gerçekleştirmesi ya da gerçekleştirmemesi üzerine algılanmış toplumsal baskıyı ifade etmektedir. Öznel normlar; yargı, inanç,

düşünce ve değerlerden oluşmaktadır. Ayrıca bireyin içinde bulunduğu toplumun gelenek, görenekleri ve sosyal yapısı ile kural ve baskılarından da öznel norm etkilenmektedir. (Davis, vd., 1989)

Algılanan Davranışsal Kontrol: Bireyin, bir davranışta bulunurken, davranış kontrolü kendine ait olmadığında, ilgili davranışı açıklamakta, davranışın kendi kontrolünde olup olmadığını algılamakta ve bunun sonucunda söz konusu davranışı gerçekleştirmenin kolaylığı ya da zorluğu hakkındaki algılamaları ifade etmekte ve davranışı gerçekleştirme noktasında karara varabilmektedir (Cibaroğlu, 2018: 39; Davis, vd., 1989)

Planlanmış davranış teorisi, teknoloji kabul modeline en çok yarar sağlayan ve teknoloji kabul modelinin açıklanmasında yardımcı olan bir teori olması ile birlikte, ani bir şekilde gelişen aşk, kavga vb. gibi sosyal psikolojik davranışlar ile düşünülmeden gerçekleştirilmiş davranışlar konusunda birçok eleştiriye maruz kalan bir teoridir (Arı ve Yılmaz, 2019: 57). Bu çerçevede kısaca planlanmış davranış teorisi için; kişilerin inançları, tavırları ve niyetleri arasında bir köprü görevi gören, kişinin söz konusu davranış konusundaki tavrı, o kişinin davranışı gerçekleştirme konusundaki niyetini ve niyeti de gerçek davranışı belirleyen ve etkileyen bir teoridir.

4.4. SDT, TKM, PDT Modellerinin Kıyaslanması

Detaylı olarak açıklanan 3 model kıyaslandığında, göreceli değerlendirmelerinin aşağıda belirtilen başlıklar altında ele alınabileceği düşünülmektedir:

4.4.1. Modelin Genel Olarak Kullanımı

TKM bilgi sistemleri/teknoloji kullanımı özelinde açılmalar getirebilmek üzere geliştirilmiş iken, SDT ve PDT ise bireylerin davranışlarını öngörmeye çalışan genel modellerdir (Podder, 2005: 38).

4.4.2. Sosyal Değişkenler

Sosyal değişkenlerin eklenmesi, modeller arasındaki bir başka farklılığı ortaya çıkarır. Keza, TKM'de sosyal değişkenler ilave edilmemişken, SDT ve PDT'de sosyal normların değişken olarak tanımlaması önem arz edebilir. İş ile ilgili yahut fayda ile ilgili sonuçlarla doğrudan ilişkilendirilmeyen sosyal etkiler olabilir ve bu durum SDT ve PDT tarafından TKM'ye göre daha başarılı bir şekilde ele alınabilir (Shumaila ve diğ., 2010: 1179).

4.4.3. Davranışsal Kontrol

TKM, algılanan kullanışlılık ve algılanan kullanım kolaylığını, bireyin bilgi sistemlerine yönelik davranış niyetlerini tahmin eden değişkenler olarak kabul ederken, TPB söz konusu kullanıcı inanışlarının duruma dayalı olduğunu ve genellenemeyeceğini söylemektedir. Bu durum PDT'ye duruma özel değişkenlerin eklenmesi avantajını sunarken, TKM'de algılanan kullanışlılık ve algılanan kullanım kolaylığı bireyin davranışını açıklamaya yönelik temel açıklayıcılar olduğundan böyle bir durum söz konusu değildir (Podder 2005, s.39).

TKM algılanan kullanım kolaylığını içsel kontrol etmenlerini açıklamak için kullanır, ancak dışsal faktörleri değerlendirmeye almaz. Buna mukabil, PDT'de, her bir durum için önem arz eden kontrol değişkenleri tanımlandığından, duruma özel faktörler daha iyi bir şekilde ele alınırlar (Shumaila ve diğ. 2010, s.1180).

4.4.4. Tahmin Etme ve Açıklama

TKM, SDT ve PDT davranışı tahmin etmek ve tanımlamak için geliştirilmişlerdir. Mezkur modellerin her biri, niyet ve davranışın açıklayıcılarını belirlerler ve değişkenler arasındaki nedensel etkilerin modelini ve yönünü detaylandırırlar. Öte yandan, tahmin etmek ve açıklamak farklı kavramlardır ve tahmin açıklamadan bağımsız olarak ortaya çıkabilirken, bu durum açıklamanın kendisi için geçerli değildir (Shumaila ve diğ. 2010, s.1180).

PDT söz konusu olduğunda bağlı dışsal değişkenlerin ve kontrol değişkenlerinin tanımlanabilmesi için önceden bir pilot araştırmaya ihtiyaç duyulurken, TKM'Nin yapısı her bir çalışmada benzer şekilde ölçülebilir. TKM tahmin etmeye yönelik bilgi sağlar, ancak yeni bir model oluşturulması için gereken bilgiyi sağlayamaz (Mathieson, 1991). Bununla birlikte, TKM sosyal herhangi bir değişken içermez (Podder 2005, s.38).

Davis (1989), SDT ve TKM'Yi kıyasladığında, TKM'Nin bir kelime işlemcisi kullanımını SDT'den daha iyi tahmin edebildiğini ortaya koymuştur. Benzer şekilde, Mathieson (1991) TKM'nin niyeti PDT'den daha iyi tahmin edebildiği sonucuna varmıştır. Bununla birlikte Taylor ve Todd (1995), TKM, PDT'ye dair yaptıkları kıyaslamada, PDT'nin niyeti daha iyi tahmin edebildiğini ortaya koymuştur (Shumaila ve diğ. 2010, s.1180).

4.4.5. Sadelik

Her üç modelin de sade olduğu söylenebilmekle birlikte, 5 değişkenden teşekkül eden TKM, 6 model içeren SDT ve 8 değişkenli PDT'ye nazaran daha sadedir (Shumaila ve diğ. 2010, s.1181).

4.5. Blok Zincir Teknolojisinin Kabulü

2018 yılında yapılan bir çalışmada blok zincir teknoloji kabul modeli 5 faktörden (güvenlik, kullanılabilirlik, güvenilirlik, çeşitlilik ve ekonomik verimlilik) oluşan bir kurulumla detaylandırılmıştır. Bu çalışmada Kore ve Vietnam'da blok zincir teknolojisinin kullanımındaki farklılıklar ele alınarak bu 5 faktörün teknolojiyi benimseyen kuruluşların üzerindeki etkisi araştırılmıştır. Elde edilen sonuçlara göre en önde çıkan faktör güvenlik olarak belirtilmiştir. Elde edilen sonuçlara göre en fazla öne çıkan 2. Faktör ise ekonomik verimlilik olarak belirlenmiştir. Çünkü blok zincir teknolojisi, merkezi bir sunucu gerektirmediğinden ve P2P dağıtılmış ağ üzerinde çalıştığından, kurulum ve bakım maliyetlerini önemli ölçüde azaltıyor. Blok zincir teknolojisinin en fazla kabul gördüğü sektör ise finans sektörüdür. (Kim, Jang, Phuong ve Gim, 2018)

Fleischmann tarafından yapılan çalışmada blok zincir teknolojisinin benimsenmesinde güven faktörü ele alınmıştır. Bu çalışma güven faktörünün hem işlevsel (ekonomik ve sistem / süreçle ilgili) hem de duygusal fayda (sosyal ve kişisel) olarak gösterildiğini ve blok zincir uygulamalarında kritik bir faktör olduğunu tanımlamıştır. Ayrıca güven faktörünün, blok zincir teknolojisini ve uygulamalarını kullanıcı / tüketici benimsemesi için anahtar bir itici güç olduğunu öne sürmektedir. (Fleischmann ve Bjoern, 2019)

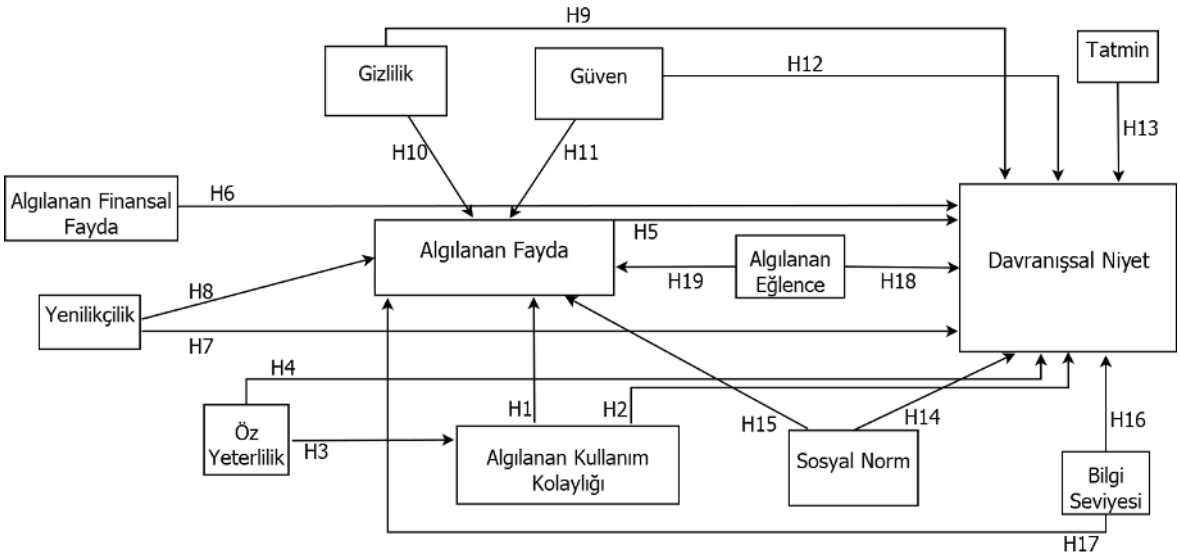
Lou tarafından gerçekleştirilen araştırmada blok zinciri teknolojisini benimsemek için süreklilik niyetini araştırmak için teknoloji kabul modelini entegre eden birleşik bir model önerilmiştir. Bu çalışmada blok zincir teknolojisini kullanma niyetlerini etkileyen en önemli faktörler olarak güven ve gizlilik faktörleri ele alınmıştır. (Lou, A.T.F., 2017)

Queiroza ve Wamba gerçekleştirdikleri çalışmada lojistik ve tedarik zinciri alanında blok zincir teknolojisinin kullanımını etkileyen faktörler teknoloji kabul modeli çerçevesinde araştırılmış ve güven, şeffaflık ve ağ aracılığıyla hesap verebilirlik, bilgi paylaşımı faktörleri incelenmiştir. Çalışmanın sonuçlarına göre blok zincir benimsenmesinde yine güven faktörü en önemli faktörlerden biri olarak gösterilmiştir. (Queiroza ve Wamba, 2019)

Knauer ve Mann blok zincir teknolojisinin tüketiciler tarafından benimsenmesini maliyet düşüklüğü, gizlilik ve sosyal ilişkiler faktörleri çerçevesinde incelenmiştir. Blok zincir teknolojisi işlem maliyetlerini azaltma, gizliliği geliştirme ve sosyal etkileşimleri yeniden tasarlama potansiyeline sahiptir ve bu da potansiyel olarak işlem ilişkilerinde tüketicinin teknolojiyi benimseme gücünü artırmaktadır. Bu üç faktörün araştırılması sonucunda tüketiciler, güvenli olarak benimsedikleri blok zincir teknolojisini, uygulamaların kullanılabilirliğindeki iyileştirmelerle düşük maliyetle kullanabileceklerine kanaat getirmişlerdir. Böylece bankalardan, teknoloji gruplarından veya bireysel devletlerden bağımsızlıklarını arttıracaklarına inanmaktadırlar. Sonuç olarak, bu teknolojinin benimsenmesindeki temel neden sadece işlem maliyetlerini düşürmesi değil, aynı zamanda güvenilir algoritmalara dayalı sistem olmasıdır. (Mann ve Knauer, 2019)

5. ARAŞTIRMANIN MODELİ

Tezin bu bölümünde önerilen araştırma modeli sunulmuştur. Bu çalışmanın temel amacı, blokzincir teknolojisinin internet bankacılığı işlemlerinde kullanımını etkileyen faktörleri belirlemektir. Bu faktörleri belirlemek için TKM temel alınmış ve güven boyutu ve teknoloji kabulü alanında araştırılan ek faktörler eklenerek genişletilmiş bir teknoloji kabul modeli oluşturulmuştur. Sunulan model Şekil 6'da verilmiştir.



Şekil 6 Araştırmanın Modeli

Sunulan araştırma modeli 2 boyuttan oluşmaktadır: TKM faktörleri ve eklenen dışsal faktörler. TKM'ne eklenen faktörler literatür taraması ile belirlenmiştir. Özelikle literatürden elde edinilen bilgilere göre blok zincir teknolojisinin benimsenmesinde güven faktörü etkin bir yapı olarak gösterilmektedir. Bu nedenle güven ve gizlilik faktörleri araştırma modelinde yer almıştır. (Kim, Jang, Phuong ve Gim, 2018; Fleischmann ve Bjoern, 2019; Lou, A.T.F., 2017; Queiroza ve Wamba, 2019; Mann ve Knauer, 2019)

Araştırma modelinde yer alan faktörler, tanımları ve ilgili hipotezler aşağıda verilmiştir:

Davranışsal Niyet (DAVNİYET): Niyet, bir şeyi yapmayı önceden isteyip düşünme, maksat olarak tanımlanmaktadır. Davranışsal niyet, kişinin söz konusu hizmeti kullanmaya yönelik niyetinin ne kadar fazla olduğunu ölçmektedir. (Davis, vd., 1989; Lai ve Li 2005; Luarn ve Lin 2005; Wang ve diğ. 2006).

Algılanan kullanım kolaylığı (AKK): Algılanan kolaylık belli bir teknolojinin kullanılmasının kolay olmasını ve fazla çaba göstermeden kullanımının öğrenilmesini ifade etmektedir. Algılanan kullanım kolaylığı, kişinin teknolojiyi kullanırken harcayacağı çabanın ne kadar az olarak algılandığını göstermektedir. (Chau ve Lai 2003; Lai ve Li 2005; Luarn ve Lin 2005; Wang ve diğ. 2006).

Bu araştırma kapsamında algılanan kullanım kolaylığı ile ilgili 2 tane hipotez öne sürülmüştür.

H_1: Bireyin algılanan kullanım kolaylığının, bireyin algılanan fayda üzerinde anlamlı etkisi vardır.

H_2: Bireyin algılanan kullanım kolaylığının, bireyin davranışsal niyeti üzerinde anlamlı etkisi vardır.

Özyeterlilik (ÖZYET): Öz yeterlilik, sosyal psikolojide önemli bir yapı olarak kişinin belli bir davranışı gerçekleştirebilme kabiliyeti olarak tanımlanmaktadır. Öz yeterlilik, kişinin belirli bir işi yapmak için gerekli kapasiteye sahip olduğuna olan inancını ifade etmektedir. (Brown ve diğ. 2003; Lassar ve diğ. 2005; Luarn ve Lin 2005; Wang ve diğ. 2006; Wang ve diğ. 2003).

Özyeterlilik faktörü ile ilgili 2 tane hipotez oluşturulmuştur.

H_3: Bireyin öz yeterliliğinin, algılanan kullanım kolaylığı üzerinde anlamlı etkisi vardır.

H_4: Bireyin öz yeterliliği, bireyin davranışsal niyeti üzerinde anlamlı etkisi vardır.

Algılanan fayda (AF): Algılanan fayda, kişinin belirli ürünü kullanarak fayda sağlayacağına inanma düzeyi olarak tanımlanabilir (Tzou, Lu, 2009). Algılanan fayda, kişinin söz konusu teknolojiyi kullanarak sağlayacağı performans artışı veya faydayı nasıl algıladığını ölçmektedir (Chau ve Lai, 2003; Davis, vd., 1989; Lai ve Li, 2005; Luarn ve Lin, 2005; Wang ve diğ. 2006).

Algılanan fayda ile ilgili bir tane hipotez oluşturulmuştur.

H_5: Bireyin algılanan faydanın, bireyin davranışsal niyeti üzerinde anlamlı etkisi vardır.

Algılanan finansal fayda(AFF): Tüketicilerin yeni teknoloji kullanımına ilişkin maliyete olan inancıdır. Söz konusu hizmetin kullanımının maliyetli olarak algılanıp algılanmadığını ölçmektedir (Hung ve Chang, 2005; Luarn ve Lin, 2005; Mathieson ve diğ. 2001). Algılanan finansal fayda ile ilgili bir tane hipotez oluşturulmuştur.

H_6: Algılanan finansal faydanın bireyin davranışsal niyeti üzerinde anlamlı etkisi vardır.

Algılanan Yenilikçilik (ALYEN): Yenilikçilik kavramı yönetim, toplum ve kültür alanlarında yeni yöntemlerin kullanılmaya başlanması anlamında kullanılmaktadır. Yenilikçilik, kişinin yeniliği diğer kişilere göre ne kadar önce benimsediğini ifade etmektedir. (Goldsmith ve Hofacker, 1991; Lassar ve diğ. 2005; Manzano ve diğ. 2009).

Algılanan yenilikçilik faktörü ile ilgili 2 tane hipotez oluşturulmuştur.

H_7: Algılanan yenilikçiliğin bireyin davranışsal niyeti üzerine anlamlı etkisi vardır.

H_8: Algılanan yenilikçiliğin, bireyin algılanan fayda üzerine anlamlı etkisi vardır.

Algılanan Gizlilik (ALGİZ): Gizlilik veya mahremiyet, bir işlem sırasında müdahil olan taraflara ait bilgilerin, işlem verilerinin ya da yazışmaların konu dışındaki kişi veya kurumlardan saklı tutulması durumu olarak tanımlanabilir. Şahsi verilerin sağlandığı elektronik ve internet gibi sanal ortamlarda bulunan verilerin korunup korunmadığı inancını ifade etmektedir (Karakaya, 2014).

Algılanan gizlilik faktörü ile ilgili 2 hipotez aşağıda verilmiştir:

H_9: Algılanan gizliliğin bireyin davranışsal niyeti üzerinde anlamlı etkisi vardır.

H_{10}: Algılanan gizliliğin bireyin algılanan fayda üzerinde anlamlı etkisi vardır.

Algılanan Güven (ALGÜVEN): Birey ya da grup ilişkilerinde karşı taraftan özveri bekleme ve bunun bireye yarar sağlayacağına inanma olarak tanımlanabilen güven, bireylerin verdikleri söz ve vaatleri yerine getireceklerine yönelik beklentidir. Bireyler tarafından algılanan güven, doğruluk ve dürüstlükle alakalı bir kavramdır (Demircan ve Ceylan, 2003; Karcıoğlu, 2013).

H_{11}: Algılanan güvenin algılanan fayda üzerinde anlamlı ve pozitif etkisi vardır.

H_{12}: Algılanan güvenin bireyin davranışsal niyeti üzerinde anlamlı ve pozitif etkisi vardır.

Algılanan Tatmin (TATMİN): Kişilerin ihtiyaç ve gereksinimlerini araştırarak bu ihtiyaçların karşılanması sonucu oluşan olumlu duygu olarak tanımlanabilir. Söz konusu uygulama veya hizmetin kullanımında bireylerin algıladıkları haz veya memnuniyeti ifade etmektedir (Brown ve diğ. 2003; Lassar ve diğ. 2005).

Tatmin faktörü ile ilgili bir tane hipotez oluşturulmuştur.

H_{13}: Bireylerin algıladıkları tatminin bireyin davranışsal niyeti üzerinde anlamlı etkisi vardır.

Sosyal Norm (SOSNORM): Sosyal norm toplum bireylerinin davranışlarını yöneten gayri anlayışlardır. Sosyal norm, ortam içerisinde gelişen genel davranış biçimleridir. (Cobb ve diğ. 1992; Özmantar ve diğ., 2009; Yackel ve Cobb, 1996)

H_{14}: Sosyal normun bireyin davranışsal niyeti üzerine anlamlı etkisi vardır.

H_{15}: Sosyal normun bireyin algılanan faydası üzerine anlamlı etkisi vardır.

Bilgi Seviyesi (BİLGİ): Online bankacılık, önemli bir benimsemeyi etkileyen faktördür. Bir tüketicinin çevrimiçi bankacılık hakkında sahip olduğu bilgi miktarı, tüketicinin çevrimiçi bankacılığı kabul etmesi üzerinde olumlu bir etkiye sahiptir (Pikkarainen ve diğ. 2004; Sathye 1999; Taylor ve Todd, 1995).

Bilgi seviyesi ile ilgili 2 tane hipotez oluşturulmuştur.

H_{16}: Bilgi seviyesinin bireyin davranışsal niyeti üzerine anlamlı etkisi vardır.

H_{17}: Bilgi Seviyesinin bireyin algılanan faydası üzerine anlamlı etkisi vardır.

Algılanan Eğlence (EĞLENCE): Algılanan eğlence, belirli bir sistemi kullanma faaliyetinin, sistemin kullanılmasından kaynaklanan performans sonuçlarının dışında, kendi içinde eğlenceli olduğu algısının derecesidir. Algılanan eğlence, bir teknolojiyi kullanırken önemli bir unsurdur (Sung ve Yun 2010; Vankatesh, 2000).

Algılanan eğlence faktörü ile ilgili 2 tane hipotez oluşturulmuştur.

H_{18}: Algılanan eğlencenin bireyin davranışsal niyeti üzerine anlamlı etkisi vardır.

H_{19}: Algılanan eğlencenin bireyin algılanan faydası üzerine anlamlı etkisi vardır.

6. YÖNTEM

Çalışma, gözlemlerin ve ölçme yöntemlerinin tekrarlanabildiği ve sayısal araştırmalar vasıtasıyla gerçekleştirildiği araştırma yöntemi olan nicel araştırma yöntemi kullanılarak gerçekleştirilmiştir. Araştırma nicel araştırma tekniklerinden olan tarama yöntemi ile gerçekleştirilmiştir. Tarama araştırmaları "Bir konuya ya da olaya ilişkin katılımcıların görüşlerinin ya da ilgi, beceri, yetenek, tutum vb. özelliklerinin belirlendiği genellikle diğer araştırmalara göre daha büyük örneklemler üzerinde yapılan araştırmalar" şeklinde ifade edilebilir (Karasar 2015, s.122). Araştırmada veriler oluşturulan ölçek ile toplanmıştır.

6.1. Evren ve Örneklem

Araştırma evrenini; Türkiye genelinde faaliyet gösteren bankaların müşterileri oluşturmaktadır. Nicel araştırma yönteminin kullanıldığı araştırmada, veriler çevrimiçi (online) anket tekniği ile toplanmıştır. Araştırmanın örneklemini internet bankacılığı kullanan basit tesadüfi yöntemle seçilen 356 kişiden oluşmaktadır. Araştırmanın örnekleminde 239 erkek 117 kadın cevap vermiştir, sorulara yanıt verenlerin yüzde 25'i 18-21 yaş arasından, yüzde 15'i 25-28 yaş arasındandır ve geneli üniversite mezunu insanlardan oluşmaktadır.

6.2. Veri Toplama Araçları

Bu araştırmada veri toplamak için demografik sorulardan ve araştırma değişkenlerini ifade eden ölçek sorularından oluşan bir anket uygulanmıştır. Ankette yer alan demografik sorular Tablo 1'de verilmiştir. Araştırma modelinde yer alan 12 değişkeni ölçmek için toplamda 45 maddeden oluşan bir ölçek hazırlanmıştır. Bu ölçek maddeleri Tablo 2'de verilmiştir. Ölçek maddeleri literatürde yer alan çalışmalardan uyarlanmıştır. İlgili çalışmaların referansları ilgili tabloda verilmiştir. Bu bölümdeki maddeler 5'li Likert Ölçek (1-Kesinlikle katılmıyorum, 2-Katılmıyorum, 3-Kararsızım, 4-Katılıyorum, 5-Kesinlikle katılıyorum) şeklinde sorulmuştur.

Tablo 1 Demografik Anket Maddeleri

Soru	**Yanıt opsiyonları**
Cinsiyet	Kadın - Erkek
Yaş	
Eğitim Durumu	Lise Ön lisans Lisans Yüksek lisans

	Doktora
Çalışıyor musunuz?	Evet - Hayır
Çalıştığınız sektör:	
Bilgisayar kullanabilme yeterliliğinizi nasıl değerlendirirsiniz?	Çok iyi İyi Orta Kötü Çok kötü
Mobil cihaz kullanıyor musunuz (Cep Telefonu, Tablet, vb.)?	Evet - Hayır
Mobil cihaz kullanabilme yeterliliğinizi nasıl değerlendirirsiniz?	Çok iyi İyi Orta Kötü Çok kötü
Mobil cihazınızı gün içinde kaç saat kullanıyorsunuz?	1 - 3 saat 3 - 6 saat 6 - 9 saat 9 saatten fazla
Gün içinde kaç saat internet kullanıyorsunuz?	1 - 3 saat 3 - 6 saat 6 - 9 saat 9 saatten fazla
Daha önce internet bankacılığı uygulaması kullandınız mı?	Evet Hayır
Cevabınız evet ise hangi uygulamayı kullandınız?	
Hangi sıklıkla internet bankacılığını kullanıyorsunuz?	( ) Her gün ( )Haftada bir kez ( )Haftada birkaç kez ( )Ayda Bir Kez
İnternet bankacılığı aracılığı ile hangi işlemleri gerçekleştiriyorsunuz?	a) ( ) Kredi kartı işlemleri (Bilgi sorma, Başvuru, Borç Ödeme) b) ( ) Fatura Ödeme ve çeşitli ödeme işlemleri (Trafik Cezaları,Üniversite) c) ( ) Hesap Hareketlerini izleme d) ( ) Hizmet ve ürünler hakkında bilgi alma e) ( ) Vergi Ödeme işlemleri f) ( ) OGS ve HGS işlemleri g) ( ) Yatırım işlemleri (Döviz, Altın) h) ( ) GSM TL yükleme işlemleri ı) ( ) Para aktarma (Havale, EFT, Döviz işlemleri) i) ( ) Vadeli/Vadesiz Kredi işlemleri (Ek Hesap Talebi, Kredi Bilgileri, Tüketici Kredisi) j) ( ) Sanal kart kullanarak alışveriş işlemleri k) ( ) Şans Oyunları için l) ( ) Bireysel Emeklilik m)( ) Sigorta (Birikim sigortası, Zorunlu

	Deprem Sigortası)
Daha önce Blok zincir teknolojisini duydunuz mu?	Evet - Hayır
İnternet bankacılığı işlemlerinizde blok zincir teknolojisini kullandınız mı?	Evet - Hayır
Hangi platformu kullandınız? :	

Tablo 2 Ölçek Tablosu

Değişken	**Ölçek Maddeleri**	**Kaynaklar**
Algılanan kullanım kolaylığı	1. İnternet bankacılığı işlemlerinde blok zincir kullanımını öğrenmek benim için kolay olacaktır. 2. İnternet bankacılığı işlemlerinde blok zincir kullanımını kolay buluyorum. 3. İnternet bankacılığı işlemlerinde blok zincir kullanımını başarmak benim için kolay olacaktır. 4. İnternet bankacılığı uygulamasında blok zincir kullanımı açık ve anlaşılırdır. 5. İnternet bankacılığı işlemlerinde blok zincir teknolojisi ile istediğim işlemleri kolaylıkla gerçekleştirebilirim.	Wang ve diğ. (2006), Luarn ve Lin (2005), Chau ve Lai (2003), Lai ve Li (2005)
Algılanan fayda	1. İnternet bankacılığı işlemlerinde blok zincir kullanarak işlemlerimi daha hızlı gerçekleştirebilirim. 2. İnternet bankacılığı işlemlerinde blok zincir teknolojisini kullanmam işlem performansımı arttırır. 3. İnternet bankacılığı işlemlerinde blok zincir teknolojini kullanmam işlemlerdeki etkinliğimi arttırır. 4. İnternet bankacılığı işlemlerinde blok zincir teknolojisini kullanmak işlemleri daha kolay gerçekleştirmemi sağlar. 5. İnternet bankacılığı işlemlerinde blok zincir teknolojisini kullanmak faydalıdır.	Wang ve diğ. (2006), Luarn ve Lin (2005), Chau ve Lai (2003), Lai ve Li (2005)
Algılanan finansal fayda	1. Blok zincir uygulamasının İnternet Bankacılığı işlemleri için gerekli programın ücretsiz sunulmasını uygun buluyorum. 2. Blok zincir uygulamasının İnternet Bankacılığı işlemleri için gerekli çalışan maliyetini uygun buluyorum. 3. Blok zincir uygulamasının İnternet Bankacılığı işlemleri için gerekli altyapı maliyetini (internet, donanım, yazılım vb.) yeterli	Luarn ve Lin (2005), Mathieson ve diğ. (2001)
Güven	1. Blok zincir uygulaması kullanılarak İnternet Bankacılığı işlemleri yapmak güvenli olacaktır. 2. İnternet Bankacılığı işlemlerinde blok zincir uygulaması kullanmada kişisel bilgilerin saklanması önemlidir. 3. Blok zincir uygulaması kullanarak İnternet Bankacılığı işlemleri yapmada güvenlik önemlidir. 4. İnternet Bankacılığı işlemlerinde blok zincir kullanımı verilerine hiç kimsenin izinsiz erişim sağlamaması benim için önemlidir.	Pikkarainen ve diğ. (2004)
Algılanan Yenilikçilik	**1.** Yeni bir teknoloji hakkında duyum aldıysam onu denemek için fırsat kollarım. **2.** Yaşıtlarım arasında güncel teknolojileri ilk keşfeden genellikle ben olurum. **3.** Yeni teknolojileri denemeyi isterim. 4. Genellikle yeni teknolojileri kullanmakta kararsız kalırım.	Lassar ve diğ. (2005), Aldas-Manzano ve diğ.(2009), Goldsmith ve Hofacker

Öz yeterlilik	1. İnternet bankacılığı işlemlerinde blok zincir uygulamasının nasıl kullanıldığını birisi gösterirse ben de blok zinciri kullanabilirim. 2. İnternet Bankacılığı işlemlerinde Blok zincir kullanımı konusunda kendime güveniyorum. 3. İnternet Bankacılığı işlemlerinde Blok zincir kullanımında beklenmedik sorunlarla karşılaştığımda nasıl davranmam gerektiğini bilirim.	Brown ve diğ.(2003), Luarn ve Lin (2005), Wang ve diğ.(2006), Wang ve diğ. (2003), Lassar ve diğ.(2005)
Algılanan Gizlilik	**1.** İnternet Bankacılığı işlemlerinde Blok zincir kullanımında kimlik doğrulama sürecinin yetkilendirilmemiş bir uygulama tarafından izlenmesi riski düşüktür. **2.** İnternet Bankacılığı işlemlerinde Blok zincir kullanımında kimlik doğrulama yöntemini kullanırken özel ve gizli bilgilerimin kötüye kullanılma riski oldukça düşüktür. 3. Blok zincir uygulaması ile kimlik doğrulama yönetimini kullanarak İnternet bankacılığı uygulamasına giriş yapmanın güvenli olduğunu düşünüyorum.	Chau ve Lai (2003)
Bilgi seviyesi	**1.** Sunulan bilginin bütünlüğü İnternet Bankacılığı işlemlerinde Blok zincir uygulamasını kullanma kararımı etkiler. **2.** Sunulan bilginin anlaşılabilirliği İnternet Bankacılığı işlemlerinde Blok zincir uygulamasını kullanma kararımı etkiler. 3. Sunulan bilginin yeterliliği İnternet Bankacılığı işlemlerinde Blok zincir uygulamasını kullanma kararımı etkiler.	Pikkarainen ve diğ. (2004)
Eğlence	1. İnternet Bankacılığı işlemlerinde Blok zincir uygulamasıyla işlem yapmak heyecan vericidir. 2. İnternet Bankacılığı işlemlerinde Blok zincir uygulaması kullanmayı seviyorum. 3. İnternet Bankacılığı işlemlerinde Blok zincir uygulaması kullanmak eğlencelidir.	Polasik ve Wisniewski (2009)
Tatmin	1. 1.Genel olarak İnternet Bankacılığı işlemlerinde Blok zincir uygulamasının sunduğu hizmetlerin kalitesinden memnunum. 2. İnternet Bankacılığı işlemlerinde Blok zincir uygulamasının modern olmasından oldukça memnunum. 3. İnternet Bankacılığı işlemlerinde Blok zincir uygulamasına erişimin kolay olmasından oldukça memnunum.	Brown ve diğ. (2003), Lassar ve diğ. (2005)
Davranışsal Niyet	1. Finansal işlemlerim söz konusu olduğunda gelecekte de İnternet Bankacılığı Blok zincir uygulaması kullanmaya niyetliyim. 2. Blok zincir uygulaması kullanılan İnternet Bankacılığı işlemlerinde meydana gelecek değişiklikleri finansal işlemlerimde uygulamaya çalışacağım. 3. İnternet Bankacılığı Blok zincir uygulaması kullanılan İnternet Bankacılığı işlemlerini yakın bir gelecekte düzenli olarak kullanmayı düşünüyorum. 4. İnternet bankacılığı işlemlerinde blok zincir kullanımını erişim olduğu sürece kullanma niyetindeyim. 5. İnternet bankacılığı işlemlerimde blok zincir kullanımına erişim olduğu sürece kullanacağımı tahmin ediyorum.	Chau ve Lai (2003), Lai ve Li (2005), Suh ve Han (2002)

Sosyal Norm	1. Çevremdeki kişiler İnternet Bankacılığı işlemlerinde Blok zincir uygulaması kullanmamın iyi bir fikir olduğunu düşünüyor. 2. Çevremdeki kişiler İnternet Bankacılığı işlemlerinde Blok zincir uygulaması kullanmam gerektiğini düşünüyor. 3. Çevremdeki kişiler beni İnternet Bankacılığı işlemlerinde Blok zincir uygulaması kullanmaya teşvik ediyor. 4. İnternet Bankacılığı işlemlerinde Blok zincir uygulaması kullanmam konusunda çevremdekiler ısrarcı olabiliyor.	Wang ve diğ. (2006), Luarn ve Lin (2005), Lai ve Li (2005), Suh ve Han (2002)

Hazırlanan veri toplama aracının güvenilirliğini ölçmek için bir pilot çalışma gerçekleştirilmiştir. Pilot çalışma 70 kişi üzerinden gerçekleşmiştir. Pilot çalışmaya 56 kişi katılmıştır. Pilot çalışmanın güvenilirlik analizi cronbach-alfa testi üzerinden gerçekleştirilmiştir. Bu teste göre alfa değerinin 0,7'den büyük olması gerekmektedir ve bu doğrultuda tüm faktörler güvenli olarak bulunmuştur (Field, 2005) (Tablo-3). Akabinde ana veri toplanması aşamasına geçilmiştir.

Tablo 3 Pilot Çalışma Güvenirlik Analizi Sonuçları

Faktör	**Madde sayısı**	**Cronbach Alfa**
TATMİN	5	,895
AF	5	,919
AFF	3	,843
AGÜVEN	4	,909
ALYEN	4	,816
ÖZYET	3	,880
AGİZ	3	,836
BİLGİ	6	,888
EGLENCE	3	,816
DAVNİYET	5	,942
SOSNORM	4	,920
AKK	3	,868

6.3. Veri toplama

Hazırlanan veri toplama aracı katılımcılara online olarak sunulmuştur. Google Forms platformunda hazırlanan ölçek linki katılımcılara iletilmiştir. Anket soruları 400 kişiye gönderilmiş, 371 kişiden yanıt alınmış cevaplar 1 ay süre içerisinde toplanmıştır.

6.4. Etik Kurul Onayı

Bu çalışma insan katılımcılar ile gerçekleştirildiği için, etik kurul onayı alınmasını gerektirmiştir. Bu nedenle Başkent Üniversitesi, Sosyal ve Beşeri Bilimler Bilimsel Araştırma ve Yayın Etiği Kurulu'ndan gerekli izinler alınmıştır. Alınan onay Ek-1'de sunulmuştur.

6.5. Araştırmanın Varsayımları

Araştırmada örneklemin evreni temsil ettiği, veri toplama araçlarının araştırmanın amacını karşıladığı ve katılımcıların ölçeklerde yer alan ifadelere yönelik belirttikleri görüşlerin doğru ve samimi olduğu varsayılmaktadır.

6.6. Verilerin Analizi

6.6.1. Açıklayıcı Faktör Analizi

Sosyal bilimlerde, araştırmacılar genellikle doğrudan ölçülemeyen şeyleri araştırırlar, böylece gözlemlenmemiş yapı hakkında soruları içeren bir anket oluşturarak araştırılan gözlenmeyen yapının farklı yönlerini araştırırlar ve daha sonra soruları azaltmak için faktör analizi uygularlar. (Field, 2005). Ayrıca faktör analizi, gözlemlenen değişkenlerden (Manifest Değişken olarak da adlandırılır) gözlemlenmemiş faktörler (bazen Gizli Değişkenler olarak adlandırılır) oluşturma fırsatı sağlar. Açıklayıcı Faktör Analizi (AFA), sosyal bilimlerde en çok kullanılan uygulamalı istatistiksel tekniklerden biridir (Costello ve Osborne, 2005).

Faktör analizinin yapılabilmesi için ilk olarak örneklemin yeterli olup olmadığını incelemek için bu analiz yapılmıştır. Temel amacı ölçülen değişkenler arasındaki temel ilişkileri tanımlamaktır.

6.6.2. Doğrulayıcı Faktör Analizi

Doğrulayıcı faktör analizi (DFA), en yaygın olarak sosyal araştırmada kullanılan özel bir faktör analizi biçimidir. Bir yapının ölçümlerinin, bir araştırmacının o yapının (veya faktörün) doğasını anlamasıyla tutarlı olup olmadığını test etmek için kullanılır. Doğrulayıcı faktör analizinin amacı, verilerin varsayılmış bir ölçüm modeline uyup uymadığını test etmektir. YEM'in özel bir uygulaması olan DFA, önceden tanımlanmış faktör yapıları için hipotezleri doğrulamak için kullanılan teoriye dayalı bir analiz yöntemidir (Albright & Park, 2009).

6.6.3. Yapısal Eşitlik Modellemesi

Teoriler, değişkenler arasındaki ilişkinin açıklamalarıdır ve sosyal bilimlerdeki çoğu teori, bu korelasyonları değişkenler arasındaki geçici ilişkiler hakkında hipotezler önermek için kullanır (Kelloway, 1998). Yapısal Eşitlik Modellemesi (YEM), gizli ve gözlenen değişkenler arasındaki ilişkileri test etmek için istatistiksel bir yöntemdir (Hoyle, 1995) ve doğrulayıcı analize dayanmaktadır (Byrne, 1998). YEM, çoğunlukla davranış bilimlerinde kullanılmaktadır (Gefen, Straub ve Boudreau, 2000). YEM'in uygulamalarında Model

Spesifikasyon, Tanımlama, Tahmin, Test Uygunluğu, Yeniden Belirleme olmak üzere 5 temel adımı vardır.

YEM'in iki tür yaklaşımı vardır: Kovaryans tabanlı YEM ve Bileşen tabanlı YEM (Gefen vd., 2000). Kovaryans tabanlı YEM, LISREL, EQS, AMOS, SEPATH, RAMONA, MX, CALIS ile yapılırken, Kısmi-En Küçük Kareler Bazlı YEM olarak da adlandırılan Kısmi En Küçük Kareler Testi (KEKKT-PC), KEKKT Grafiği ile bileşen bazlı YEM gerçekleştirilmektedir. Bu iki yaklaşım, hedeflerinde, analizdeki varsayımlarda ve uyum istatistiklerinde değişir.

Bu tez kapsamında Kısmi En Küçük Kareler Testi(KEKKT) esaslı YEM uygulanmıştır.

6.6.4. Kısmi En Küçük Kareler Testi Yol Modellemesi

KEKKT yol modelini tanımlamak için bir ölçüm ve yapısal bir model kullanılır. Bir ölçüm modeli, gizli değişkenler ile açık değişkenler arasındaki ilişkileri gösterirken, yapısal bir model gizli değişkenler arasındaki ilişkileri temsil eder (Chatelin, Vinzi ve Tenenhaus, 2002). Ölçüm modeli için, faktörleri doğrulamak için yakınsak ve ayırt edici geçerlilik kullanılır. Yakınsamayı doğrulamak için, her bir madde gizli değişkenini anlamlı bir t değeri ile sonuçlandırmalıdır (Gefen ve Straub, 2005). Ortalama Çıkarılan Varyans (AVE) skoru analiz edildiğinde ayırt edici geçerliliği gösterir; her gizli değişken için AVE puanının karekökü, herhangi bir gizli değişken çiftinin korelasyonundan daha büyük olmalıdır (Gefen & Straub, 2005).

Bu çalışmada, ölçüm ve yapısal modelleri tasarlamak için SmartPLS kullanılmıştır. SmartPLS, YEM'i tasarlamak için bir araçtır (Ringle, Wende, Will, 2005). SmartPLS'de oluşturulan modeller Kısmi En Küçük Kareler analizi ile ölçülür (Hansmann & Ringle, 2004).

7. BULGULAR

Bu bölümde istatiksel veri analizi sonuçları verilmiştir. Daha sonra açıklayıcı ve doğrulayıcı faktör analizi sonuçları ile birlikte yapısal model sunulmuştur.

7.1. Demografik Özelliklere Dair Bulgular

İlk önce katılımcıların demografik özellikleri SPSS Amos 26 ile analiz edilmiştir. Demografik bulgular ve ön analiz sonuçları Ek-2'de verilmiştir. Katılımcılara demografik olarak 17 tane soru sorulmuştur. Bunların analiz sonuçlara göre katılımcılar cinsiyetlerine göre %67,1 (239 Kişi) Erkek, %32,9 (117 Kişi) Kadın şeklinde dağılım göstermiştir.

Katılımcılar yaşlarına göre %48,3 (172 Kişi) 21-30 Yaş, %20,2 (72 Kişi) 20 yaş ve altı, %13,8 (49 Kişi) 31-40 Yaş, %9,3 (33 Kişi) 51 yaş ve üzeri ve %8,4 (30 Kişi) 41-50 Yaş şeklinde dağılmıştır. Katılımcılar eğitim durumlarına göre %60,7 (216 Kişi) lisans, %22,5 (80 Kişi) yüksek lisans, %9,8 (35 Kişi) doktora ve %7 (25 Kişi) lise şeklinde dağılmıştır. Katılımcıların %53,4'ü (190 kişi) hali hazırda çalıştıklarını, %46,6'sı (166 Kişi) ise herhangi bir işte çalışmadıklarını belirtmişlerdir. Katılımcılar bilgisayar kullanabilme yeteneklerine göre %38,5'i (137 Kişi) iyi, %33,4'ü (119 Kişi) çok iyi, %26,4'ü (94 Kişi) orta ve %1,7'si (6 Kişi) kötü şeklinde dağılmıştır. Katılımcılar mobil cihaz kullanabilme yeteneklerine göre %50,8 (181 Kişi) iyi, %40,2 (143 Kişi) çok iyi, %8,4 (30 Kişi) orta ve %0,6 (2 Kişi) kötü şeklinde dağılmıştır. Katılımcıların mobil cihazları gün içinde kullanım sürelerine göre dağılımına bakıldığında %44,4'ü (158 Kişi) 3-6 Saat, %24,4'ü (87 Kişi) 6-9 Saat, %19,1'i (68 Kişi) 1-3 Saat ve %12,1'i (43 Kişi) 9 saat ve üzeri şeklinde dağılmıştır. Katılımcıların interneti gün içinde kullanım sürelerine göre dağılımına bakıldığında %31,5'i (112 Kişi) 6-9 Saat, %29,8'i (106 Kişi) 9 saat ve üzeri, %27'si (96 Kişi) 3-6 Saat ve %11,8'i (42 Kişi) 1-3 saat şeklinde dağılmıştır. Katılımcıların %98,3'ü daha önce internet bankacılığını kullandığını, %1,7'si ise daha önce internet bankacılığını kullanmadığını belirtmiştir. Katılımcıların %39,6'sı (141 kişi) haftada bir kez, %25'i (89 Kişi) haftada birkaç kez, %21,6'sı (77 kişi) her gün ve %13,8'i (49 Kişi) ayda bir kez internet bankacılığını kullandıklarını belirtmişlerdir. Katılımcıların daha önce blok zincir teknolojisi kullanma durumlarına göre dağılımına bakıldığında %52,5'i (187 Kişi) evet, %47,5'i (169 Kişi) hayır cevabını vermiştir. Katılımcıların internet bankacılığı işlemlerinde blok zincir teknolojisini kullanma durumlarına göre dağılımına bakıldığında %95,5'i (340 Kişi) hayır, %4,5'i (16 kişi) evet şeklinde dağılmıştır.

7.2. Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları

Açıklayıcı faktör analizi IBM SPSS Amos 26 ile gerçekleştirilmiştir. Faktör analizinin yapılabilmesi için ilk olarak örneklemin yeterli olup olmadığını incelemek için Kaiser-Mayer-Olkin (KMO) Testi yapılmıştır. KMO test sonucunun 0.5 değerinden büyük olması incelenmek ele alınan verilerin örneklem boyutunun yeterli olduğunu göstermektedir (Kalaycı, 2010, s. 322). Daha sonra verilerin faktör analizi için uygun olup olmadığının test edilmesi gerekmektedir. Bunun için ise Barlett' s Sphericity Test kullanılmaktadır. Bu test sonucunda elde edilen p değerinin 0.05' den küçük olması verilerin faktör analizi için uygun olduğunu göstermektedir. Analiz sonucunda elde edilen KMO ve Barlett Testi sonuçları aşağıdaki gibidir;

Tablo 4 KMO Barlett Küresellik Testi

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,933
Bartlett's Test of Sphericity	Approx. Chi-Square	9544,454
	df	496
	Sig.	,000

Blok Zincir Teknolojisi Kullanımına dair araştırmada kullanılan veri toplama aracından elde edilen verilere uygulanan KMO Küresellik testi ve Barlett's testi sonuçlarına göre verilerin analiz uygun olduğu tespit edilmiştir.

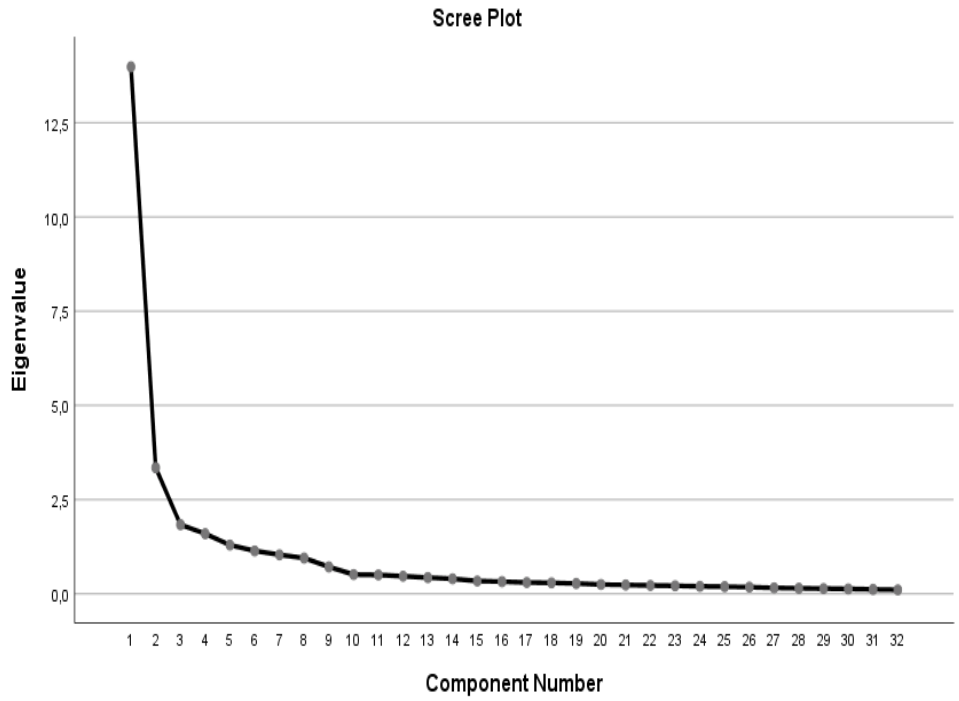
Faktör analizi sonucunda elde edilen faktörlerin özdeğerleri ve açıklanan varyans oranları Tablo 5'te gösterilmiştir.

Tablo 5 Elde edilen faktörlerin özdeğerleri ve açıklanan varyans oranları

Faktörler	Özdeğerler	Açıklanan Varyans	Toplam Varyans
1	13,981	43,690	43,690
2	3,346	10,458	54,148
3	1,835	5,733	59,881
4	1,595	4,983	64,864
5	1,293	4,041	68,905
6	1,138	3,557	72,462
7	1,035	3,235	75,697
8	,949	2,965	78,661
9	,714	2,232	80,894

Yapılan faktör analizi sonucunda toplam varyansın %80.894'ünü açıklayan 9 faktörlü bir yapı elde edilmiştir. Varimax dönüşümü yapıldıktan sonra, faktör yük değerleri incelenmiştir.

Faktör analizinin faktör yüklerinden oluşan Şekil 7'de kaç adet faktör olduğu hakkında çıkarımda bulunmak mümkündür. 9 adet faktörün gösterildiği şekil aşağıdaki gibidir.



Şekil 7 KMO Barlett Küresellik Testi

Faktör analiz sonuçlarını incelemek için faktör yükleri önem taşımaktadır. Analiz sonucunda elde edilen faktör yükleri Tablo 6'da gösterilmiştir.

Tablo 6 Açıklayıcı Faktör Analizi

	1	2	3	4	5	6	7	8	9	**Cronbach's Alpha**
DNIY40	,731									
DNIY41	,689									
DNIY38	,666									
DNIY39	,664									
DNIY37	,644									0.942
SOSNORM44		,880								
SOSNORM43		,829								
SOSNORM42		,754								
SOSNORM45		,743								0.920
AF9			,814							
AF7			,767							
AF8			,753							
AF6			,629							
AF10			,462							0.919
AGUVEN16				,874						
AGUVEN15				,824						
AGUVEN17				,799						0.909
AYEN20					,783					
AYEN18					,736					
AYEN19					,588					0.818
AKK3						,782				0.869

AKK1	,724				
AKK2	,576				
BILGI29		,796			
BILGI30		,680			
BILGI28		,619			0.888
AGIZ26			,767		
AGIZ25			,566		
AGIZ27			,565		0.837
TATMİN36				,672	
TATMİN35				,630	
TATMİN34				,530	0.895

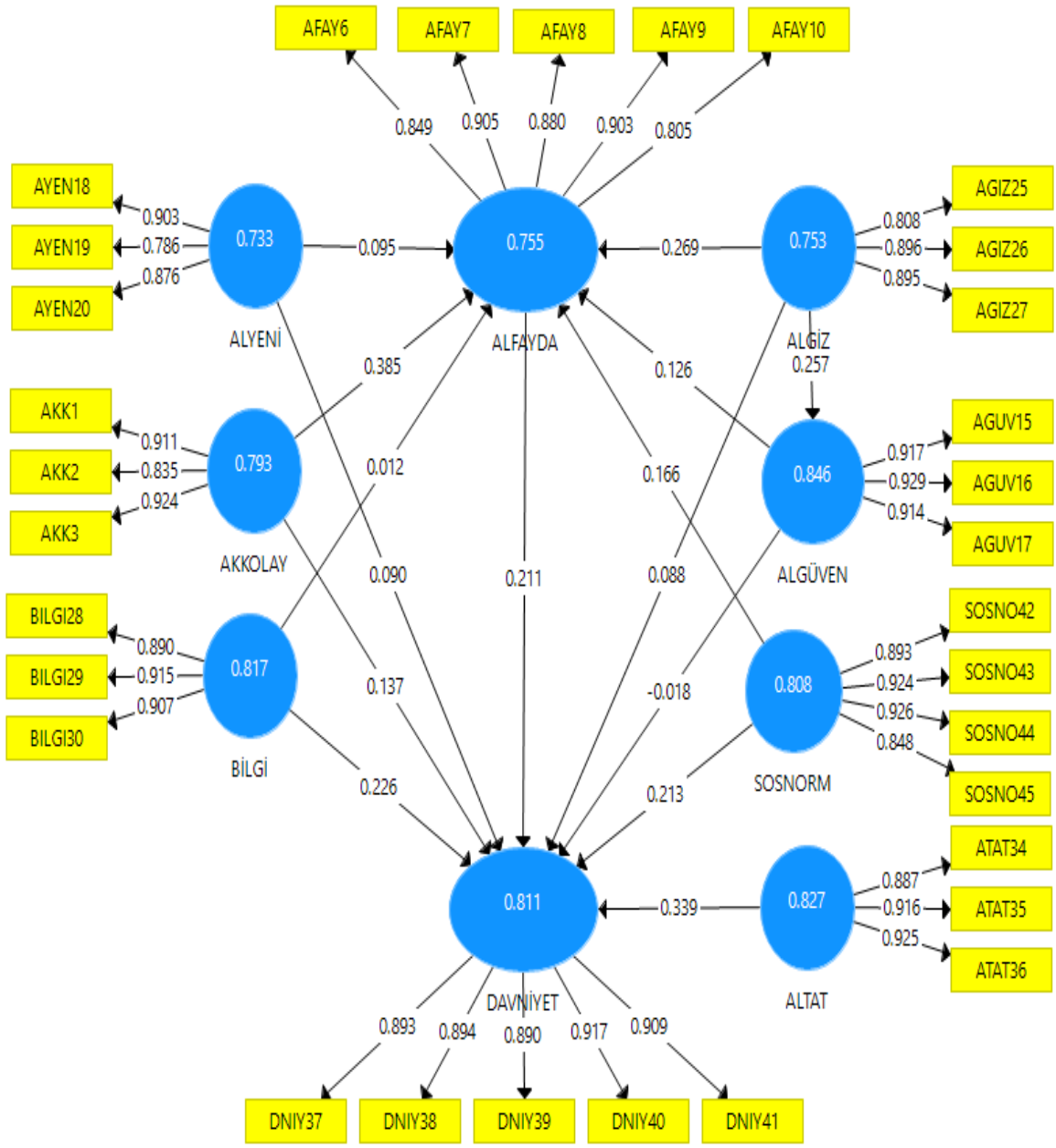
Açıklayıcı Faktör analizinde anlamsal bütünlük sağlayan ve faktör yükleri 0.4 ve üzeri olanlar ele alınmıştır. Ayrıca Yamaç Grafiği incelemesinde eğimin değişme durumuna göre cümlelerin 9 faktör altında toplanmasının uygun olduğu görülmüştür. TABLO 6'da 9 faktör ve bunların yükleri ile güvenirlik sonuçları verilmiştir. Tablodan da görüldü gibi bütün faktör yükleri 0.4'ün üzerindedir. Bütün faktörler cronbach alfa değerine göre güvenilir olarak bulunmuştur (bütün cronbach alfa değerleri 0,7'nin üzerindedir). (Field,2005)

7.3. Doğrulayıcı Faktör Analizi

Ölçüm modelini değerlendirmek için doğrulayıcı faktör analizi gerçekleştirilmiştir. Doğrulayıcı Faktör Analizi bir yapının ölçümlerinin, bir araştırmacının o yapının (veya faktörün) doğasını anlamasıyla tutarlı olup olmadığını test etmek için kullanılır. Doğrulayıcı faktör analizinin amacı, verilerin varsayılmış bir ölçüm modeline uyup uymadığını test etmektir.

Ölçüm modeli değerlendirilmesi yakınsak geçerlilik ve ayırt edici geçerlilik ile değerlendirilir. Yakınsak geçerlilik için faktör yükleri, bileşik güvenilirlik ve çıkarılan ortalama varyans (composite reliability ve average variance extracted) değerleri değerlendirilmiştir.

Ölçüm modeli: Ölçüm modelini oluşturmak için SmartPLS kullanılmıştır. Ölçüm modeli Şekil 8'de verilmiştir.



Şekil 8 Ölçüm Modeli

7.3.1. Yakınsak Geçerliliği (Convergent validity):

Faktör yükleri: Yakınsak geçerliliği **(convergent validity)** sağlamak için faktör yüklerinin 0.7'den büyük olması gerekmektedir. Faktör yükleri Tablo 7'de verilmiştir. Bütün faktör yükleri 0,7'den büyüktür.

Tablo 7 Faktör Yükleri Tablosu

	DNIY	TATMİN	BİLGİ	AKK	SOSNORM	ALGÜVEN	ALYEN	AF	ALGİZ
DNIY37	0,893								
DNIY38	0,894								
DNIY39	0,890								
DNIY40	0,917								
DNIY41	0,909								
TATMİN34		0,887							
TATMİN35		0,916							
TATMİN36		0,925							
BILGI28			0,890						
BILGI29			0,915						
BILGI30			0,907						
AKK1				0,911					
AKK2				0,835					
AKK3				0,924					
SOSNORM42					0,893				
SOSNORM43					0,924				
SOSNORM44					0,926				
SOSNORM45					0,848				
AGUVEN15						0,917			
AGUVEN16						0,929			
AGUVEN17						0,914			
ALYEN18							0,903		
ALYEN19							0,786		
ALYEN20							0,876		
AF10								0,805	
AF6								0,849	
AF7								0,905	
AF8								0,880	
AF9								0,903	
AGIZ25									0,808
AGIZ26									0,896
AGIZ27									0,895

Bileşik güvenilirlik(Composite Reliability): Bileşik güvenilirlik sonuçlarının 0,7'den yüksek olması gerekmektedir. Tablo 8'de bileşik güvenilirlik sonuçları verilmiştir. Tabloda görüldüğü gibi bütün faktörler bileşik güvenilirliği sağlamaktadır.

Çıkarılan Ortalama Varyans (AVE): AVE sonuçları 0,5'ten büyük olmalıdır. Bütün faktörlerin AVE değerleri Tablo 8'de verilmiştir. Tablodan da görüldüğü gibi bütün faktörler gerekli AVE değerini sağlamaktadır.

Tablo 8 Bileşik Güvenilirlik Sonuçları

Faktör	Bileşik Güvenilirlik	AVE
AKK	0,920	0,793
AF	0,939	0,755
ALGÜVEN	0,943	0,846
AGİZ	0,901	0,753
TATMİN	0,935	0,827
ALYEN	0,892	0,733
BİLGİ	0,931	0,817
DAVNİYET	0,955	0,811
SOSNORM	0,944	0,808

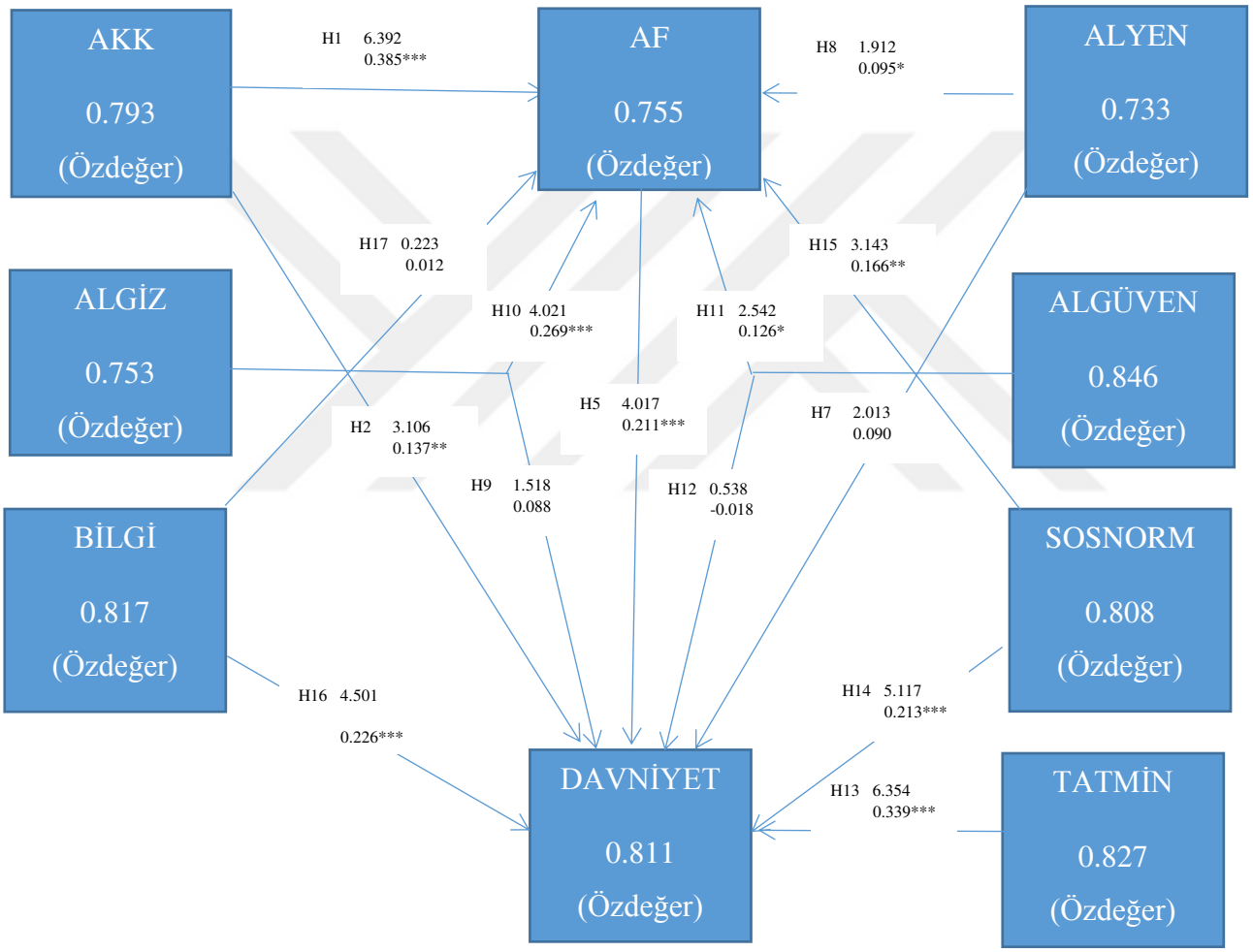
7.3.2. Ayrımcı Geçerlilik (Discriminant validity):

Ayrımcı geçerlilik bütün faktörlerin birbirinden farklı olduğunu göstermek için gerçekleştirilir. Fornell & Larcker (1981) ve Gefen & Straub (2005), yapılar arası korelasyon dikkate alınarak ayırt edici geçerliliğin değerlendirildiğini belirtmiştir. Her yapının AVE değerlerinin karekökü, yapıların tüm korelasyon değerlerinden daha yüksek olmalıdır. Tablo 9'da ayrımcı geçerliliğin sonuçları verilmiştir. Sonuçlar bütün faktörlerin AVE karekökü değerlerinin korelasyonlardan yüksek olduğunu göstermektedir. Tablo 9'da ayrımcı geçerlilik sonuçları verilmiştir. Sonuçlar bütün faktörlerin birbirinden farklı olduğunu göstermektedir.

Tablo 9 Ayrımcı Geçerlilik Sonuçları

	AKK	AF	AL GÜVEN	ALGİZ	TATMİN	ALYEN	BİLGİ	DAVNİYET	SOSNORM
AKK	**0,891**								
AF	0,638	**0,869**							
ALGÜVEN	0,362	0,366	**0,920**						
ALGİZ	0,446	0,572	0,257	**0,868**					
TATMİN	0,464	0,630	0,259	0,626	**0,910**				
ALYEN	0,506	0,479	0,276	0,424	0,411	**0,856**			
BİLGİ	0,479	0,476	0,536	0,518	0,435	0,454	**0,904**		
DAVNİYET	0,545	0,686	0,300	0,626	0,738	0,498	0,578	**0,900**	
SOSNORM	0,289	0,436	0,047	0,513	0,556	0,294	0,279	0,577	**0,899**

Yapısal model: Ölçüm modeli ayrımcı geçerlilik(discriminant validity) ve bileşik güvenilirlik (convergent validity) ile doğrulandıktan sonra KEKKT ön yükleme (bootstrapping) algoritması ile faktörler arasındaki ilişkileri değerlendirmek için t değerleri hesaplanmıştır. Şekil-9'da doğrulanan yapısal model verilmiştir. Şekilde oklar üzerinde yol katsayıları ile t skorları verilmiştir. Tek yönlü oklar regresyonları temsil etmektedir. Okların üzerindeki rakamlardan üstteki rakamlar t değerini, alttaki rakamlar regresyon katsayısını temsil etmektedir. Bu minvalde ilişkiler figür üzerinden anlamlandırılmaktadır ve geçerli kılınmıştır.



*p<0.005 **p<0.01 ***p<0.001

Şekil 9 Yapısal Model

7.4. Hipotez testi sonuçları

İlişkilerin sonuçları ve test edilen hipotez sonuçları Tablo 10'da verilmiştir. Açıklayıcı faktör analizinde özyeterlilik, algılanan finansal fayda ve eğlence faktörlerini ölçen maddeler düzgün dağılım göstermediği için sonraki analizlerde kullanılmamıştır. Bu nedenle bu faktörlerle ilişkili olan H3, H4, H18 ve H19 hipotezleri test edilememiştir.

Elde edilen sonuçlara göre H7, H9, H12 ve H17 hipotezleri reddedilmiştir. H1, H2, H5, H8, H10, H11, H13, H14, H15, H16 hipotezleri desteklenmiştir.

Tablo 10 İlişkiler ve hipotez testi sonuçları

İLİŞKİLER	HİPOTEZ	T Değerleri	Standardize Değerler	DESTEKLEME
AKK ---> AF	**H1**	6,392	0,385***	Evet
AKK ---> DAVNİYET	H2	3,106	0,137**	Evet
ÖZYET ---> AF	H3			Ölçülemedi
ÖZYET ---> DAVNİYET	H4			Ölçülemedi
AF ---> DAVNİYET	H5	4,017	0,211***	Evet
AFF ---> DAVNİYET	H6			Ölçülemedi
ALYEN ---> DAVNİYET	H7	2,013	0,090	Hayır
ALYEN ---> AF	H8	1,912	0,095*	Evet
ALGİZ ---> DAVNİYET	H9	1,518	0,088	Hayır
ALGİZ ---> AF	H10	4,021	0,269***	Evet
ALGÜVEN ---> AF	H11	2,542	0,126*	Evet
ALGÜVEN ---> DAVNİYET	H12	0,538	-0,018	Hayır
TATMİN ---> DAVNİYET	H13	6,354	0,339***	Evet
SOSNORM ---> DAVNİYET	H14	5,117	0,213***	Evet
SOSNORM ---> AF	H15	3,243	0,166**	Evet
BİLGİ ---> DAVNİYET	H16	4,501	0,226***	Evet
BİLGİ ---> AF	H17	0,223	0,012	Hayır
EĞLENCE ---> DAVNİYET	H18			Ölçülemedi
EĞLENCE ---> AF	H19			Ölçülemedi

*p<0.005 **p<0.01 ***p<0.001

8. TARTIŞMA

Bu bölümde ampirik analizler sonucunda elde edilen sonuçlar tartışılmaktadır. Bu çalışma TKM modelini temel alıp, dışsal faktörler ile genişletip bir blokzincir kabul modeli doğrulamıştır. Önerilen yapısal model, blokzincir teknolojisinin internet bankacılığı işlemlerinde blokzincir teknolojisinin kullanımına karşı davranışsal niyeti etkileyen faktörleri açıklamaktadır.

Kullanıcıların yeni bir bilgi sistemine yönelik tutumlarının ve kabul edilmesinin, başarılı bilgi sistemi benimseme üzerinde kritik bir etkiye sahip olduğu belirtilmiştir (Davis, 1989; Venkatesh ve Davis, 1996; Succi ve Walter, 1999). Kullanıcılar bilgi sistemini kabul etmeye istekli değilse, bu, kuruma tam fayda sağlamayacaktır (Davis, 1993; Davis ve Venkatesh, 1996). Kullanıcılar yeni bir bilgi sistemini ne kadar kabul ederlerse, uygulamalarında değişiklik yapmaya ve yeni bilgi sistemini fiilen kullanmaya başlamak için zamanlarını ve çabalarını kullanmaya o kadar isteklidirler (Succi ve Walter, 1999).

Bilgi sistemi kabulü çalışmasında en çok kullanılan modellerden biri, sistemin içinde bulunduğu teknoloji kabul modelidir (TKM (Davis vd., 1989; Mathieson, 1991; Davis ve Venkatesh, 1996; Gefen ve Straub, 2000; Al Gahtani, 2001). Kullanım (gerçek davranış), niyet ve son olarak davranışla ilgili kullanıma yönelik tutumla ilgili algılanan fayda (AF) ve algılanan kullanım kolaylığı (AKK) tarafından belirlenir. Bu çalışma kapsamında Teknoloji Kabul Modeli Faktörlerinden algılanan fayda, algılanan kullanım kolaylığı ve davranışsal niyet faktörleri ele alınmıştır. İnternet bankacılığı işlemlerinde halihazırda blokzincir kullanan yeterli katılımcıya ulaşmanın zor olacağı öngörüldüğünden davranışsal niyet faktörü bağımlı değişken olarak düşünülmüş ve kullanıcıların internet bankacılığı işlemlerinde blokzincir kullanımını belirleyici değişken olarak olarak ele alınmıştır. Bu çalışma kapsamında TKM faktörlerine ek olarak, algılanan yenilikçilik, algılanan gizlilik, algılanan güven, tatmin, sosyal norm, ve bilgi seviyesi faktörleri doğrulanmıştır.

Ampirik sonuçlardan elde edilen bulgulara göre, algılanan kullanım kolaylığı algılanan fayda ve davranışsal niyet faktörlerini anlamlı şekilde etkilemektedir. Bu değişkenler arasında pozitif ilişki bulunmuştur. Yani kullanıcılar blok zincir teknolojisinin kullanımını kolay bulurlarsa, kullanıma karşı davranışsal niyetleri ve fayda algıları pozitif etkilenecektir. Elde edilen bu sonuç geçmiş çalışmalar ile paraleldir (Davis, 1989; Davis vd., 1989; Mathieson, 1991; Adams vd., 1992; Davis, 1993; Segars ve Grover, 1993; Taylor ve Todd, 1995).

Elde edilen sonuçlar ile algılanan fayda ve davranışsal niyet arasında pozitif ve anlamlı bir ilişki bulunmuştur. Bu sonuç TKM modeli ile paraleldir (Mathieson, 1991; Davis ve Venkatesh, 1996). Bu ilişkiye göre eğer kullanıcılar blok zincir teknolojisini faydalı bulursa, internet bankacılığında blok zincir kullanımına karşı davranışsal niyetleri artacaktır.

Elde edilen sonuçlara göre algılanan yenilikçilik ve algılanan fayda faktörleri arasındaki ilişki pozitif ve anlamlı olarak belirlenmiştir. Bu ilişkiden elde edilen sonuca göre yeni teknolojileri denemeye meyillli olan kişilerin internet bankacılığı işlemlerinde blokzincir teknolojisini kullanma niyetleri artacaktır (Davis, 1989; Davis vd., 1989; Mathieson, 1991)

İnternet bankacılığının hızla yaygınlaşması, tüm ticari iş ve işlemlerin mobil bankacılık üzerinden gerçekleşmesi, sanal kart ve kredi kartı kullanımını ve e- ticaret sitelerinin yaygınlaşmasıyla insanlar neredeyse tüm parasal işlemlerini internet bankacılığı üzerinden gerçekleştirmektedir. Bu alanda yapılan siber saldırıların artması, kredi kartı bilgilerinin çalınması, hesapların ele geçirilmesi kullanıcılar için ciddi maddi kayıplara ve mağduriyetlere neden olmuştur. Blok zincir teknolojisinin arka planındaki mimarinin izlenememesi ve güvenlik katsayısını artırması nedeniyle internet bankacılığı kullanımında, insanlar bankacılık işlemlerinin gizliliğine inanmaktadır. Bu çalışmada da algılanan gizlilik ve algılanan fayda arasındaki ilişki anlamlı olarak bulunmuştur (Succi ve Walter, 1999). Bu sonuç blokzincir teknolojisinin gizlilik sağladığına karşı inançlarının güçlü olduğunu ve bunun fayda algılarını pozitif yönde etkilediğini göstermektedir.

Elde edilen sonuçlara göre, yenilikçi teknolojiler ve blok zincir teknolojisi insanların internet bankacılığı kullanımına duydukları güveni artırmıştır. Para transferleri, banka hesap bilgileri gibi süreçleri mahrem olarak görenler, güven algısını blok zincir teknolojisinin arttırdığını düşünmektedir. Bu çalışmada da algılanan güven ve algılanan fayda arasındaki ilişki incelendiğinde pozitif ve anlamlı olduğu görülmektedir. (Davis, 1989; Venkatesh ve Davis, 1996; Succi ve Walter, 1999). Bu sonuç kişilerin blokzincir teknolojisini güvenli bulduklarını ve bundan dolayı da faydalı bulduklarını ima etmektedir.

Tüm sistemlerde olduğu gibi, insanlar yeni bir teknoloji veya uygulama ile karşılaştığında, yeniliğin sağlayacağı faydaları ve kazanımları değerlendirmektedir. Yeni teknolojilerin faydalarını tecrübe ettikçe ve deneyimledikçe, pozitif etkilerinden doygunluk

seviyesine ulaşınca kullanıcılar o teknolojiye yönelimi ve yönlendirmesi hızla artmaktadır. Dolayısıyla, ampirik sonuçlardan da elde edilen bulgulara göre, insanlar blok zincir teknolojisinin faydalı ve elverişli bir şekilde kullanımı noktasında kullanıcılar tatmin olursa, bu teknolojiyle internet bankacılığı kullanımına karşı davranışsal niyeti ve kullanım oranı pozitif ve anlamlı bir şekilde etkilenecektir. (Davis, 1993; Davis ve Venkatesh, 1996).

Şüphesiz insanlar çevresinden ve sosyal hayatındaki arkadaşlarından birçok konuda etkilenmektedir. Çevrenin yapmış olduğu pozitif algı, insanların yeni bir teknolojiyi kullanmasını veya kullanmamasını ciddi oranda etkilemektedir. Elde edilen bulgulara göre, Sosyal norm faktörü ile algılanan fayda ve davranışsal niyet arasında pozitif ve anlamlı ilişki tespit edilmiştir. Bu değişkenler arasında internet bankacılığında blok zincir teknolojisinin kullanımına yönelik çevresinin oluşturduğu pozitif algı, çevresinin bu teknolojiye duyduğu güven ve yarattığı pozitif etkiden ötürü kullanıcılarda güvenlik, gizlilik vb. konulardan fayda sağlayacağı görüşünden hareketle, insanların bu teknolojiyi kullanma niyeti artmaktadır. (Succi ve Walter, 1999).

Elde edilen sonuçlara göre, internet bankacılığında blok zincir teknolojisinin kullanımıyla ilgili insanların bilgi seviyesi ne kadar yüksekse, insanlar bu teknolojiyi ne kadar tanıyor ve özelliklerini biliyorsa, kullanma eğilimi o kadar artmaktadır. Yenilikçi teknolojilere ve blok zincir teknolojisinin pozitif etkilerine vakıf olma durumu, kullanıcıları bu teknolojiyi bankacılık işlemlerinde kullanmaya meylettirmektedir. Dolayısıyla bilgi seviyesi ve davranışsal niyet arasındaki ilişki pozitif ve anlamlıdır. (Davis vd., 1989; Mathieson, 1991; Davis ve Venkatesh, 1996; Gefen ve Straub, 2000; Al Gahtani, 2001).

9. SONUÇ

Finansal sistemlerde işlemler güvene dayalı olarak gerçekleştirilmektedir. Geleneksel yapıda güven, işlemleri gerçekleştiren tarafların arasında bulunan aracı kurumlar tarafından sağlanmaktadır. Aracı kurumların işlemleri her zaman tarafların çıkarına yapmama ya da bilgileri dâhilinde olmadan gerçekleştirme riskleri bulunmaktadır. Mevcut risklere ilaveten 2008 yılında yaşanan finansal kriz ile tarafların aracı kurumlara olan güveni büyük oranda sarsıntıya uğramıştır. Blok zinciri teknolojisi, finansal kurumlara olan güvenin sarsıldığı bu kriz ortamında ortaya çıkmıştır. 2008 yılında Satoshi Nakamoto tarafından yayınlanan makale ile tarafların güven ihtiyacına çözüm olarak sunulan blok

zinciri teknolojisi tanıtılmıştır. Blok zinciri teknolojisi, işlemlerin eşten eşe aracısız olarak gerçekleştirilmesine imkân tanımaktadır. İşlemler gerçekleştirilirken aracıların ortadan kaldırılmasıyla tarafların güven ihtiyacı karşılanırken aynı zamanda maliyet ve zaman tasarrufu yapmaları sağlanmaktadır.

Blok zinciri teknolojisinin sağlamış olduğu avantajlar bunlarla sınırlı değildir. Blok zinciri teknolojisinde işlemler kötü niyetli müdahalelere karşı değişmez olarak kaydedilmektedir. Veri bütünlüğünü korumanın önemli olduğu alanlarda verilerin değişmez olarak kaydedilmesi büyük bir avantajdır. Blok zincirine kaydedilen veriler herkese açık ve şeffaftır. Böylelikle yapılan her işlem açıklanmakta ve sistemin sağladığı güven duygusu pekişmektedir. Ayrıca verilerin dağıtık defter teknolojisi ile kaydediliyor oluşu da sisteme duyulan güveni artırmaktadır. Blok zinciri teknolojisinin potansiyeli henüz keşfedilme aşamasındadır. Kullanım alanı oldukça geniş olan bu yeni teknoloji, günümüzde kullanılan merkezi, internet tabanlı mimarinin aksine, eğer şifresi çözülürse olumsuz sonuçlara neden olacak merkezi bir sunucu ihtiyacını ortadan kaldırır.

Blok zincir teknolojisi veri hırsızlığı, kimlik avı saldırıları ve diğer siber saldırı türlerini engellemek için ve efektif çözümler sunmak için kullanılabilir. Mimarisi gereği dağınık otoriteye dayalı bir kimlik doğrulama sistemi ve dağıtık dijital veri tabanı sayesinde doğrulama sistemlerinde güvenlik tehditlerine karşı alınabilecek tedbirlerin en başarılısı konumundadır. Dolayısıyla kimlik doğrulama sistemlerinde verimli bir şekilde kullanılabilir. Gelişmiş şifreleme teknolojilerine sahip bu teknoloji, alt yapısı sayesinde kimlik hırsızlığının önüne geçebilir ve kullanıcıların özel anahtarlarını ve verilerini talep etmeden doğrulama yapabilir. Böylece kimlik doğrulamak için dağıtılmış açık anahtar altyapısı kullanılmasını da sağlamaktadır.

Bu teknolojinin güçlü DNS giriş yaklaşımı, her cihaz için şifre yerine belirli bir SSL sertifikası sağlaması, sertifika verileri bu teknoloji ile yönetildiğinde sahte sertifika kullanımının da önüne geçmektedir. Dolayısıyla finans sektöründe para transferinin diğer sektörlerde veri paylaşımının güvenliğini artırmak için kullanılabilir.

Blok zincirin dağıtılmış defter teknolojisi ile tüm bilgiler açık bir şekilde belirli bir zincirin üyeleri tarafından kullanılabilir. Bu zincirdeki şifreli veriler üye düğümleri tarafından okunabilir ve dağıtılabilir. Böylece bulut ortamlarda şirketlerin ortak hareket etmesine fayda sağlayabilir. Kimlik yönetimi, şifreli mesajlar ve veri şifreleme gibi birçok alanda da kullanılabilir. Bu teknoloji bulut bilişim dâhil tüm ağı kapsayacak şekilde güvenli veri depolamayı, işlem ve hesap yapmayı sağlar.

Bu teknoloji kimlik doğrulama alanında da kullanılabiliyor. Oluşturulan dijital kimlik sayesinde yetkili kurumlar tarafından kimlik doğrulanabiliyor ve başvuru gibi süreçlerde kullanılabiliyor.

Sağlık sektöründe kritik öneme sahip sağlık bilgilerinin bu teknoloji üzerinden sigorta şirketleri ile paylaşılmasında, medikal kayıtların ve ilaç kullanım bilgilerinin sağlık kurumları arasında paylaşılmasında ve sahte bilgi dolaşımının engellenmesinde kullanılabilir.

Dolayısıyla sağlamış olduğu avantajlar ile sadece finans sektörünün değil finansal olmayan sektörlerin mevcut iş süreçlerini de iyileştirecek birçok çözümü bünyesinde barındırmaktadır.

Bu bilgilerden hareketle, yapmış olduğumuz çalışmanın sonuçlarını derleyecek olursak; yapmış olduğumuz çalışma neticesinde 9 adet anlamlı faktör bulunmuştur. Bu faktörlerin hepsi internet bankacılığında blok zincir teknolojisinin kullanımını pozitif yönde etkilemekte ve kullanıcıları bu teknolojiyi kullanma ve yaygınlaştırma noktasında etkilemektedir.

İnsanlar yeni bir teknoloji veya uygulama ile karşılaştığında ilk etapta kullanım kolaylığı noktasında tereddüde düşebilirler. Çünkü insanlar bilmediği şeylerden korkarlar. Kullanıcıların bir yenilik karşısındaki bilgi seviyeleri ne kadar yüksekse kullanım oranları o ölçüde artmaktadır. Bununla beraber, kullanıcılar bu teknolojinin kolay bir şekilde kullanılacağını, bu teknolojiye hızlı adapte olacağına inanırlarsa ve bu teknolojiden fayda ve kazanım elde edeceğini bilirlerse hızlı bir şekilde teknolojiyi kullanır ve benimserler. Sosyal psikolojide kişinin belirli bir davranışı gerçekleştirme kapasitesi bir yeniliği benimsemesini de etkilemektedir. Yani bir kullanıcı kendini yeni bir teknolojiyi kullanma noktasında yeterli görürse kullanma niyeti de pozitif yönde etkilenecektir.

Yenilikçilik kavramı yönetim, toplum ve kültür alanlarında yeni yöntemlerin kullanılmaya başlanması anlamında kullanılmaktadır. Blok zincir teknolojisi de internet bankacılığında çok yeni ve kullanımı henüz yaygınlaşmamış bir teknolojidir. Teknoloji ne kadar çok kullanılırsa ve yaygınlaşırsa, çevresinden etkilenen ve kullanımının arttığını gözlemleyen kullanıcıların bu yeni teknoloji üzerindeki davranışsal niyeti o oranda pozitif olarak etkilenecektir.

Son olarak, bu teknolojinin kullanımını en çok etkileyen husus gizlilik ve mahremiyet sağlayıp sağlamamasıdır. Bir işlem sırasında müdahil olan taraflara ait

bilgilerin, işlem verilerinin ya da yazışmaların konu dışındaki kişi veya kurumlardan saklı tutulması, kişisel verilerin internet gibi sanal ortamlarda korunup korunmadığı inancı, maddi ve manevi zarara karşı koruma duygusu ve insanların bu teknolojiye duymuş oldukları güven kullanıcıların davranışsal niyeti üzerinde ki en önemli faktörlerdir. Dolayısıyla gizlilik, güven faktörleri yeni gelişmekte olan blok zincir teknolojisinin internet bankacılığında kullanımı noktasında kritik öneme haizdir.

KAYNAKÇA

Abubakar, A., Shagari, J.N., Olusegun, K.L. (2015). The Relationship Between Electronic Banking And Liquidity Of Deposit Money Banks In Nigeria, *International Journal of Economics, Commerce and Management.*

Adams, D.A., Nelson, R.R. and Todd, P.A. (1992), "Perceived usefulness, ease of use, and usage of information technology: a replication", MIS Quarterly, June, pp. 227-47.

Albright, J. J., & Park, H. M. (April, 2009). Confirmatory Factor Analysis using Amos, LISREL, Mplus, SAS/STAT CALIS. Retrieved from http://www.indiana.edu/~statmath/stat/all/cfa/cfa.pdf.

Ajzen I. (1991). *The Theory of Planned Behavior*, Organizational Behavior and Human Decision Processes, 50, 179-211.

Ajzen, I. and Fishbein, M. (1980), Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Englewood Cliffs, NJ.

Ajzen, I. and Madden, T. (1986). *Prediction of goal directed behaviour: Attitudes, intentions and perceived behavioural control*.

Akça, C. (2005), *Microsoft'tan Anti-Casus Yazılımı: Windows AntiSpyware* http://www.pclabs.gen.tr/2005/01/07/microsofttan-anticasus-yazilimi-windows-antispyware/

Akın, M. (2007). *Sanal Hizmetlerde Hizmet Kalitesi,* Gazi Kitabevi, Ankara.

Al-Gahtani, S. (2001), "The applicability of TAM outside North America: an empirical test in the United Kingdom", Information Resources Management Journal, JulySeptember, pp. 37-46.

Alipour, J. (2016) "Factors Affectıng Hospıtal Informatıon System Acceptance By Caregıvers Of Educatıonal Hospıtals Based On Technology Acceptance Model (Tam): A Study In Iran"

Altınışık, F. (2000). Şimdi Online Bankacılık Moda, *Bankacılık Dergisi:* Dünya Dosyaları.

Androulaki, E. (2018). Hyperledger Fabric: A Distributed Operating System For Permissioned Blok zincirs, *In Proceedings of the Thirteenth EuroSys Conference,* 30-35.

Atik, E. (2015). *Turizmde Akıllı Telefon Kullanımının Teknoloji kabul modeli Kapsamında Değerlendirilmesi*. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Turizm İşletmeciliği Anabilim Dalı, Yüksek Lisans Tezi.

Ayıgulıaılı, A. (2016). *İnternet Bankacılığının Başarısını Etkileyen Faktörlerin Tespiti: Türkiye ve Çin Karşılaştırması,* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Barışık, S. ve Temel, H. (2007). İnternet Bankacılığı Kullanımında Güvenlik Unsurlarının Bilinirliği, *Dergi Park /Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi,* 2, 140-145.

Bayoğlu, S. (2010). *Türkiye'de İnternet Bankacılığı Adaptasyonunu Etkileyen Faktörlerin Teknoloji-Organizasyon-Çevre Modeli İle Araştırılması,* Yayımlanmamış Doktora Tezi, T.C. Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Bayraktar, Ş. (2019). *Bilgi uzmanlarının bilgi teknolojisi kullanımının teknoloji kabul modeli ile incelenmesi*, Burdur Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Üniversitesi, Yüksek Lisans Tezi, Burdur.

Byrne, B. M. (1998). Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS. New Jersey: Lawrence Erlbaum Associates, Publishers.

Cachin, C. (2016). Architecture Of The Hyperledger Blok zincir Fabric, *In Workshop On Distributed Cryptocurrencies And Consensus Ledgers,* 310-315.

Cocco, L., Pınna, A. ve Marchesı, M. (2017). *Banking On Blockchain: Costs Savings Thanks to the Blockchain Technology*, Future Internet, 9 (25), 5.

Compeau, R.D. and Higgins, A.C. (1995), "Computer selfefficacy: development of a measure and initial test", MIS Quarterly, Vol. 19 No. 2, pp. 189-211.

Cronin, M. (1998)." *Banking and Finance on the Internet",* John Wiley and Sons, New York.

Çankaya, S. (2012), Finansal Yönetim Dersi, *Nakit Yönetimi dersnotları*, http://kampus.beykent.edu.tr/Paylasim/Dosyalar/8.hafta_129806 173005830000.pdf

Çakar, M.M., 2018, "Girişimcilerin Bilgi Teknolojilerini Kullanma Nedenlerinin Teknoloji Kabul Modeli Kapsamında Analizi: Manisa İli Örneği", Yüksek Lisans Tezi

Çelik, A. (2018). *Eğitim Fakültesi Öğrencilerinin Dijital Ürünlerle İlgili Telif Hakları Konusundaki Farkındalık Düzeylerinin İncelenmesi*, Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.

Cibaroğlu, M.O. (2018), "Elektronik Belge Yönetim Sistemlerinin Genişletilmiş Teknoloji Kabul Modelinin Temelinde Kullanımı: Ampirik Bir Değerlendirme", Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi.

Costello, A. B. & Osborne, J. W. (2005). Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most From Your Analysis. Practical Assessment, Research & Evaluation, 10 (7).

Chatelin, Y. M., Vinzi, V. E., Tenenhaus, M. (2004). State–of–art on PLS path modeling throug the aviable software. HEC Research paper series CR 764.

Davis, F. D., (1989). *Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology*, MIS Quarterly, 13 (3): 319-340.

Davis, F.D. (1993), "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts", International Journal of Man-Machine Studies, Vol. 38, pp. 475-87.

Davis, F.D. and Venkatesh, V. (1996), "A critical assessment of potential measurement biases in the technology acceptance model: three experiments", International Journal of Human-Computer Studies, Vol. 45, pp. 19-45.

Dayıoğlu, B. (2017), *Ağ ve İşletim Sistemleri*, http://www.e-ticaretmerkezi.net/agveisletimsistemi.pdf

DeLone, W.H. and McLean, E.R. (1992), "Information systems success: the quest for the dependent variable", Information Systems Research, Vol. 3 No. 1, pp. 60-95.

Demirdöğmez, M. (2018). Türkiye'de E-Ticaret Sektörünün Yıllara Göre Gelişimi, *Uluslararası Toplum Araştırmaları Dergisi-International Journal of Society Researches.*

Durbilmez, S.E. (2018). *Blok zincir Teknolojisinin Finans Sektöründeki Yeri Ve Uygulamaları,* Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Erdem, H. K. (2011). *Kurumsal kaynak planlama sistemlerinin kullanımında etkili olan faktörlerin genişletilmiş teknoloji kabul modeli ile incelenmesi* (Yayımlanmamış doktora tezi). İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Erdem, A. ve Efiloğlu, Ö. (2002). *Bilgi Çağında Elektronik Ticaret,* 8. Türkiye'de İnternet Konferansı, İstanbul.

Eroğlu, N. ve Yücel, İ.Z. (2012). Türkiye'deki Kurumsal Banka Müşterilerinin İnternet Bankacılığı Kullanım Eğilimlerini Belirleyen Başlıca Faktörler Üzerine Amprik Bir Çalışma, Marmara Üniversitesi, *Bankacılık ve Sigortacılık Enstitüsü E-Dergisi,* 2(2), 10-14.

Erten, S. (2002). Planlanmış davranış teorisi ile uygulamalı öğretim metodu. Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 19(2), 217-233.

Fangfang, D., Yue, S., Nan, M., Liang, W., Zhiguo, Y. (2017). From Bitcoin to Cybersecurity: a Comparative Study of Blok zincir Application and Security Issues. The 2017 4th International Conference of Systems and Informatics (ICSAI 2017), 975-979.

Fishbein, M. ve Ajzen, I. (1975). *İnanç, Tutum, Niyet ve Davranış: Teori ve Araştırmaya Giriş*. Okuma, MA: Addison-Wesley.

Field, A. (2005). Discovering Statistics Using SPSS. London: Sage Publications.

Martin Fleischmann, M. And Ivens, B.S. (2019), "Exploring the Role of Trust in Blockchain Adoption:An Inductive Approach: Proceedingsofthe52ndHawaiiInternationalConferenceonSystemSciences"

Gefen, D. and Straub, D. (2000), "The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption", Journal of the Association for Information Systems, Vol. 1 No. 8, pp. 1-28.

Guo, Y. and Liang, C. (2016). *Blockchain application and outlook in the banking industry*. Financial Innovation, 2(1), 24.

Gutu, L.M. (2014). *The İmpact Of İnternet Technology On The Romanian Banks Performance,* 12th International Academic Conerence, Prague.

Hansmann, K-W., & Ringle, C. M. (2004, August 13). SmartPLS Manuel. Retrieved from http://www.ibl-unihh.de/manual.pdf.

Hassani, V., Crasta, N. and Pascoal, A.M. (2017). *Cyber security issues in navigation systems of marine vessels from a control perspective*. In: Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering - OMAE. New York City: American Society of Mechanical Engineers.

Henderson, R. and Divett, M. (2003), "Perceived usefulness, ease of use and electronic supermarket use", International Journal of Human-Computer Studies, Vol. 59 No. 3, pp. 383-95.

Horvitz, P.M. (1996). Preserving Competition in Electronic Home Banking, *Journal of Money,* 971-946.

Hoyle, R. H. (1995). Structural Equation Modeling Concepts, Issues and Applications. USA: Sage Publications California.

İleri, Y.Y. (2011). Effects Of İnternet Banking And E-Commerce On Turkish Economy, *Selçuk University Journal of Social Sciences Vocational School,* 1, 109-126.

Kara, Ö. (2002). Bankacılıkta Akıllı Kart Uygulamaları". Türkiye Bilişim Derneği, *Bilişim Kültür Dergisi*, 82, 13-25.

Karaköse, İ.S. (2017). *Elektronik Ödemelerde Blok Zinciri Ve Sistematiği Ve Uygulamaları,* Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Kayseri.

Kelloway E. K. (1998). Using LISREL for Structural Equation Modeling A Researcher's Guide. London: Sage Publications.

Kılıç, Y. (2015). Ele*ktronik Ticaret Kullanımında Tüketicilerin Tercihlerini Etkileyen Faktörler*. Türk Hava Kurumu Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Knauer F.O., Mann A. (2019) "What is in It for Me?Identifying Drivers of BlockchainAcceptance among German Consumers, 8-10"

Koskosas, İ. (2011). The Pros and Cons of Internet Banking: A Short Review, *Business Excellence and Management,* 1(1), 49-58.

Krause, E.G., Velamuri, V. K., Burghardt, T., Nack, D., Schmidt, M. and Treder, T. M. (2016). *Blockchain Technology and the Financial Services Market State-of-the-Art Analysis*, HHL, 6.

Lu, J., Yu, C.S., Liu, C. and Yao, J.E. (2003), "Technology acceptance model for wireless Internet", Internet Research, Vol. 13 No. 3, pp. 206-22.

Lou, Antonio T. F. and Li, Eldon Y., "Integrating Innovation Diffusion Theory and the Technology Acceptance Model: The adoption of blockchain technology from business managers' perspective" (2017). ICEB 2017 Proceedings. 44.

Mathieson, K. (1991). *Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior*. Information Systems Research, 2(3), 173-191.

Maciel M. Queiroz, Samuel Fosso Wamba, Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA, International Journal of Information Management, Volume 46, 2019, Pages 70-82.

Miller, A.Y. (2016). *The Honey Badger Of BFT Protocols,"* İn Proceedings Of The, Conference on Computer and Communications Security, Vienna, Austria.

Onay, C. ve Ozsoz, E. (2012). T*he Impact of Internet-Banking on Brick and MortarBranches: The Case of Turkey*, Journal of Financial Services Research 44(2):187-204.

Ortunç, Y. (2003). *Türk Bankacılık Sektöründe Elektronik Bankacılık ve Sayısal Analizi,* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Öztürk, Ö. (2006). *Müşteri İlişkileri Yönetimi ve İnternet Bankacılığı Üzerine Bir Uygulama*, Yüksek Lisans Tezi, İstanbul.

Pazvant, E. (2017). *Nesnelerin İnterneti Teknolojisine Sahip Ürünlerin Kullanım Niyetinin Teknoloji Kabul Modeli Kapsamında Değerlendirilmesi*. Düzce Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Yüksek Lisans Tezi.

Pikkarainen,T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer Acceptance of Online Banking: An Extension of the Technology Acceptance Model. Internet Research, 14(3): 224-235.

Pisa, M. and Juden, M. (2017). *Blockchain and Economic Development: Hype vs. Reality*. CGD Policy Paper. Washington, DC: Center for Global Development. Available at: https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality.

Polatoğlu, V. N. ve Ekin, S. (2001). An Empirical İnvestigation of the Turkish Consumers Acceptance of İnternet Banking Services, *International Journal of Bank Marketing,* 19(4), 156-165.

Podder, B. (2005), "Factors Influencing the Adoption and Usage of ınternet Banking: A New Zealand Perspective", Master Thesis of Information Technology at the Auckland University of Technology.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0 (beta), www.smartpls.de.

Rogers, E. M. (1995). *Diffusion of innovations* (4th edition). The Free Press. New York.

Sathye, M. (1999), "Adoption of Internet banking by Australian consumers: an empirical investigation", International Journal of Bank Marketing, Vol. 17 No. 7, pp. 324-34.

Segars, A.H. and Grover, V. (1993), "Re-examining perceived easy of use and usefulness: a confirmatory factor analysis", MIS Quarterly, December, pp. 517-25.

Seyhan, H. (2019). *İnovatif Bankacılık Ürünleri Kullanımının Teknoloji Kabul Modeli İle İncelenmesi*, Nevşehir Hacı Bektaş Veli Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Nevşehir.

Shumaila, Y. Y., (2010), "Explaining Internet Banking Behavior: Theory of Reasoned Action, Theory of Planned Behavior, or Technology Acceptance Model?"

Sousa, J. (2018). *A byzantine Fault-Tolerant Ordering Service For The Hyperledger Fabric Blok zincir Platform,* In 2018 48th Annual IEEE/IFIP İnternational Conference On Dependable Systems And Network, 51-58.

Stoica, O. (2015). The İmpact Of İnternet Banking On The Performance Of Romanian Banks: DEA and PCA Approach, *Procedia Economics and Finance,* 20, 610-622.

Succi, M.J. and Walter, Z.D. (1999), "Theory of user acceptance of information technologies: an examination of health care professionals", Proceedings of the 32nd Hawaii International Conference on System Sciences (HICSS), pp. 1-7.

Sullivan, R.J. (2000). How Has The Adoption of Internet Banking Affected Performance And Risk İn Banks, Federal Reserve Bank of Kansas City, *Financial Industry Perspectives,* 1-16.

Şamlı, R. ve Yüksel, E. (2009). Biyometrik Güvenlik Sistemleri, XI. *Akademik Bilişim Konferansı Bildirileri,* Şanlıurfa.

Şen, Ö. (2017). *Online Alışverişte Satın Alma Davranışının Planlı Davranış Teorisi, Teknoloji Kabul Modeli*, *Yenilik Yayılım Kuramı, Tüketici Alışkanlıkları ve Güven Faktörleriyle İncelenmesi*, Haliç Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul.

Kim, S.S., Jang W.J. , Phuong H.T., Gim G.Y. (2018) "A Comparative Study on the Intention of Using Blockchain Technology in Korea and Vietnam"

Taylor, S. and Todd, P.A. (1995), "Understanding information technology usage: a test of competing models", Information Systems Research, Vol. 6 No. 2, pp. 144-76.

Tekeli, E. (2015), http://glokalweb.com/2015/03/22/internet-bankaciligi-ve-mobil-bankaciligin-tarihsel-gelisimi/

Venkatesh, V. and Davis, F.D. (2000), "Theoretical extension of the technology acceptance model: four longitudinal field studies", Management Science, Vol. 46 No. 2, pp. 186-204.

Venkatesh, V. and Speier, C. (1999), "Computer technology training in the workplace: a longitudinal investigation of the effect of mood", Organizational Behavior and Human Decision Processes, Vol. 79, pp. 1-28.

Venkatesh, V., Speier, C. and Morris, M.G. (2002), "User acceptance enablers in individual decision making about technology: toward an integrated model", Decision Sciences, Vol. 33 No. 3, pp. 297-316.

Weiser, E. B. (2001). *The functions of internet use and their social and psychological consequences*. Cyberpsychology & Behavior, 4 (6), 723-743.

Yazıcı, S. (2014). *E-Öğrenme: İnsan Kaynakları Eğitiminde Stratejik Dönüşüm,* Alfa Basım, İstanbul.

Yerlikaya, S. (2017). *Seçilmiş Avrupa Birliği Ülkeleri ve Türkiye'de Dijital Bankacılığın Dönüşümü,* Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, İstanbul.

Yıldırım, K. (2006). *Elektronik Bankacılık-Avrupa Birliği ve Türkiye Uygulamaları,* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Yılmaz, E. (1999). Akıllı Kartlar, *Banka ve Para Teknolojileri Dergisi* 1, 5-15.

Yurttadur, M. ve Süzen, E. (2016). Türkiye'de Banka Müşterilerinin İnternet Bankacılığına Yaklaşımlarının İncelenmesi Üzerine Bir Uygulama, *Tüketici ve Tüketim Araştırmaları Dergisi,* 8(1), 95-99.

Yücel, İ.S. (2012). *Türkiye'deki Kurumsal Banka Müşterilerinin İnternet Bankacılığı Eğilimleri, İSİDEF Üzerine Bir Uygulama,* Yayımlanmamış Doktora Tezi, T.C. Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, İstanbul.

Zeren, D. (2018). *Teknoloji Kabul Modeli*. M. İ. Yağcı ve S. Çabuk içinde, Pazarlama Teorileri (s. 171-186). İstanbul: Kapital Medya Hizmetleri A.Ş.

EKLER

EK-1: Etik Kurul Onayı

Sayı : 17162298.600-397
Konu : Tez Çalışması

11 MAYIS 2020

İlgili Makama

Üniversitemiz Sosyal Bilimler Enstitüsü Teknoloji ve Bilgi Yönetimi Tezli Yüksek Lisans Programı öğrencisi Abdulkerim Oğuzhan Alkan'ın, Dr. Öğretim Üyesi Nurcan Alkış'ın danışmanlığında yürütmekte olduğu "İnternet Bankacılığında Blok Zincir Teknolojisinin Kullanımını Güvenlik Bakış Açısıyla Değerlendirmek" başlıklı yüksek lisans tez çalışması değerlendirilmiş ve yapılmasında bir sakınca olmadığı tespit edilmiştir.
Bilgilerinize saygılarımızla sunarız.

Başkent Üniversitesi Sosyal ve Beşeri Bilimler ve Sanat Araştırma Kurulu

Ad, Soyad	Değerlendirme	İmza
Prof. Dr. M. Abdülkadir Varoğlu	Olumlu/~~Olumsuz~~	
Prof. Dr. Kudret Güven	Olumlu/Olumsuz	
Prof. Ali Sevgi	Olumlu/Olumsuz	
Prof. Dr. Işıl Bulut	Olumlu/Olumsuz	
Prof. Dr. Sadegül Akbaba Altun	Olumlu/~~Olumsuz~~	
Prof. Dr. Can Mehmet Hersek	Olumlu/~~Olumsuz~~	
Prof. Dr. Özcan Yağcı	Olumlu/~~Olumsuz~~	

EK-2: Demografik Bulgular

Tablo 1. Cinsiyete Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Kadın	117	32,9	32,9	32,9
	Erkek	239	67,1	67,1	100,0
	Total	356	100,0	100,0	

Katılımcılar cinsiyetlerine göre %67,1 (239 Kişi) Erkek, %32,9 (117 Kişi) Kadın şeklinde dağılım göstermiştir.

Tablo 2. Yaşa Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	20 Yaş ve Altı	72	20,2	20,2	20,2
	21-30 Yaş	172	48,3	48,3	68,5
	31-40 Yaş	49	13,8	13,8	82,3
	41-50 Yaş	30	8,4	8,4	90,7
	51 Yaş ve üzeri	33	9,3	9,3	100,0
	Total	356	100,0	100,0	

Katılımcılar yaşlarına göre %48,3 (172 Kişi) 21-30 Yaş, %20,2 (72 Kişi) 20 yaş ve altı, %13,8 (49 Kişi) 31-40 Yaş, %9,3 (33 Kişi) 51 yaş ve üzeri ve %8,4 (30 Kişi) 41-50 Yaş şeklinde dağılmıştır.

Tablo 3. Eğitim Durumuna Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Lise	25	7,0	7,0	7,0
	Lisans	216	60,7	60,7	67,7

	Yüksek Lisans	80	22,5	22,5	90,2
	Doktora	35	9,8	9,8	100,0
	Total	356	100,0	100,0	

Katılımcılar eğitim durumlarına göre %60,7 (216 Kişi) lisans, %22,5 (80 Kişi) yüksek lisans, %9,8 (35 Kişi) doktora ve % 7 (25 Kişi) lise şeklinde dağılmıştır.

Tablo 4. Çalışma Durumlarına Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Evet	190	53,4	53,4	53,4
	Hayır	166	46,6	46,6	100,0
	Total	356	100,0	100,0	

Katılımcıların %53,4'ü (190 kişi) hali hazırda çalıştıklarını, %46,6'sı (166 Kişi) ise herhangi bir işte çalışmadıklarını belirtmişlerdir.

Tablo 5. Bilgisayar Kullanma Yeteneklerine Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Kötü	6	1,7	1,7	1,7
	Orta	94	26,4	26,4	28,1
	İyi	137	38,5	38,5	66,6
	Çok İyi	119	33,4	33,4	100,0
	Total	356	100,0	100,0	

Katılımcılar bilgisayar kullanabilme yeteneklerine göre %38,5'i (137 Kişi) iyi, %33,4'ü (119 Kişi) çok iyi, %26,4'ü (94 Kişi) orta ve %1,7'si (6 Kişi) kötü şeklinde dağılmıştır.

Tablo 6. Mobil Cihaz Kullanma Yeteneklerine Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Kötü	2	,6	,6	,6
	Orta	30	8,4	8,4	9,0
	İyi	181	50,8	50,8	59,8
	Çok İyi	143	40,2	40,2	100,0
	Total	356	100,0	100,0	

Katılımcılar mobil cihaz kullanabilme yeteneklerine göre %50,8 (181 Kişi) iyi, %40,2 (143 Kişi) çok iyi, %8,4 (30 Kişi) orta ve %0,6 (2 Kişi) kötü şeklinde dağılmıştır.

Tablo 7. Mobil Cihazları Gün İçinde Kullanım Sürelerine Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	1-3 Saat	68	19,1	19,1	19,1
	3-6 Saat	158	44,4	44,4	63,5
	6-9 Saat	87	24,4	24,4	87,9
	9 Saat ve Üzeri	43	12,1	12,1	100,0
	Total	356	100,0	100,0	

Katılımcıların mobil cihazları gün içinde kullanım sürelerine göre dağılımına bakıldığında %44,4'ü (158 Kişi) 3-6 Saat, %24,4'ü (87 Kişi) 6-9 Saat, %19,1'i (68 Kişi) 1-3 Saat ve %12,1'i (43 Kişi) 9 saat ve üzeri şeklinde dağılmıştır.

Tablo 8. İnterneti Gün İçinde Kullanım Sürelerine Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	1-3 Saat	42	11,8	11,8	11,8
	3-6 Saat	96	27,0	27,0	38,8
	6-9 Saat	112	31,5	31,5	70,2
	9 Saat ve Üzeri	106	29,8	29,8	100,0
	Total	356	100,0	100,0	

Katılımcıların interneti gün içinde kullanım sürelerine göre dağılımına bakıldığında %31,5'i (112 Kişi) 6-9 Saat, %29,8'i (106 Kişi) 9 saat ve üzeri, %27'si (96 Kişi) 3-6 Saat ve %11,8'i (42 Kişi) 1-3 saat şeklinde dağılmıştır.

Tablo 9. İnterneti Bankacılığını Kullanma Durumlarına Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Evet	350	98,3	98,3	98,3
	Hayır	6	1,7	1,7	100,0
	Total	356	100,0	100,0	

Katılımcıların %98,3'ü daha önce internet bankacılığını kullandığını, %1,7'si ise daha önce internet bankacılığını kullanmadığını belirtmiştir.

Tablo 10. İnterneti Bankacılığını Kullanma Sıklıklarına Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Ayda Bir Kez	49	13,8	13,8	13,8
	Haftada Birkaç Kez	89	25,0	25,0	38,8
	Haftada Bir Kez	141	39,6	39,6	78,4
	Her Gün	77	21,6	21,6	100,0

	Total	356	100,0	100,0	

Katılımcıların %39,6'sı (141 kişi) haftada bir kez, %25'i (89 Kişi) haftada birkaç kez, %21,6'sı (77 kişi) hergün ve %13,8'i (49 Kişi) ayda bir kez internet bankacılığını kullandıklarını belirtmişlerdir.

Tablo 11. Daha Önce Blok Zincir Teknolojisi Kullanma Durumlarına Göre Dağılım

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Evet	187	52,5	52,5	52,5
	Hayır	169	47,5	47,5	100,0
	Total	356	100,0	100,0	

Katılımcıların daha önce blok zincir teknolojisi kullanma durumlarına göre dağılımına bakıldığında %52,5'i (187 Kişi) evet, %47,5'i (169 Kişi) Hayır cevabını vermiştir.

Tablo 12. İnternet Bankacılığı İşlemlerinde Blok Zincir Teknolojisini Kullanma Durumlarına Göre

		Frekans	Yüzde	Değişken Yüzde	Kümülatif Yüzde
Valid	Evet	16	4,5	4,5	4,5
	Hayır	340	95,5	95,5	100,0
	Total	356	100,0	100,0	

Katılımcıların internet bankacılığı işlemlerinde blok zincir teknolojisini kullanma durumlarına göre dağılımına bakıldığında %95,5'i (340 Kişi) hayır, %4,5'i (16 kişi) evet şeklinde dağılmıştır.