T.C.
NİĞDE ÖMER HALİSDEMİR ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANABİLİM DALI

KRİPTO PARA VE ŞİFRELEME TEKNOLOJİSİ: EKONOMETRİK VERİ ANALİZİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Ecem TURGUT

Niğde
Temmuz, 2020

T.C.
NİĞDE ÖMER HALİSDEMİR ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANABİLİM DALI

KRİPTO PARA VE ŞİFRELEME TEKNOLOJİSİ: EKONOMETRİK VERİ ANALİZİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Ecem TURGUT

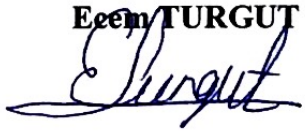
Danışman: Doç. Dr. Okyay UÇAN
Üye : Prof. Dr. Fatih YÜCEL
Üye : Dr. Öğr. Üyesi Ayşe ERGİN ÜNAL

Niğde
Temmuz, 2020

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum **"Kripto Para ve Şifreleme Teknolojisi: Ekonometrik Veri Analizi"** başlıklı bu çalışmanın, bilimsel ve akademik kurallar çerçevesinde tez yazım kılavuzuna uygun olarak tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. 14/ 07/ 2020

Ecem TURGUT



ÖNSÖZ

"Kripto Para ve Şifreleme Teknolojisi: Ekonometrik Veri Analizi" adlı bu çalışma 2020 yılında yüksek lisans tezi olarak hazırlanmıştır. Yüksek lisans tezinin amacı olarak kripto paraların kavramsal boyutu ve teorik altyapısının anlaşılması ve ekonomik etkisinin analiz edilmesi amaçlanmıştır. Bu doğrultuda kripto para ve döviz kuru ilişkisi zaman serisi yöntemi aracılığıyla sınanmış ve bir sonuca ulaşılmaya çalışılmıştır.

Çalışmanın planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın Doç. Dr. Okyay UÇAN hocama sonsuz teşekkürlerimi sunarım. Hayatımın her alanında olduğu gibi eğitim hayatımın bu aşamasında da en büyük destekçim olan ve bana inanan aileme de teşekkür ederim.

Ecem TURGUT

ÖZET
YÜKSEK LİSANS TEZİ

KRİPTO PARA VE ŞİFRELEME TEKNOLOJİSİ:
EKONOMETRİK VERİ ANALİZİ

TURGUT, Ecem
İktisat Anabilim Dalı
Tez Danışmanı: Doç. Dr. Okyay UÇAN
Temmuz 2020, 190 Sayfa

Kripto paralar, dünya ekonomisinde Bitcoin ile adını duyurmaya başlamıştır. İlk başlarda hakkında çok fazla bilgi sahibi olunmayan Bitcoin'in zaman içerisinde popülaritesi giderek artmış ve işlem hacmi daha da önemli boyutlara ulaşmıştır. Ayrıca kripto paraların getiri oranlarının çok yüksek ve işlem maliyetlerinin çok az olmasının da etkisiyle gün geçtikçe Bitcoin'in karşısına Ethereum, Litecoin, Ripple, Dash, Neo, Monero gibi farklı rakipler çıkmaya başlamıştır. Böylelikle bu şifreli para birimleri döviz piyasasında önemli bir yer almıştır. Çalışmada bu bağlamda kripto para ve döviz kuru ilişkisi analiz edilmiştir. Analizde Bitcoin bağımlı değişken; Euro, İngiliz Sterlini, Avustralya Doları, Japon Yeni, Kanada Doları, İsviçre Frangı ve Çin Yuanı gibi piyasada en çok işlem gören majör para birimleri bağımsız değişken olarak ele alınmıştır. Değişkenlerin ise 2013-2019 dönemi aylık verilerinden yararlanılmış ve Amerikan Doları karşısındaki çapraz kur değerleri kullanılmıştır. Eşbütünleşme ilişkisini analiz etmek için ARDL analizi yapılmış ve değişkenler arasında uzun dönemli bir ilişki saptanamamıştır. Akabinde VAR analizi kapsamında uygulanan cusum testi sonucunda değişkenlerin güvenli bir bant aralığında olduğu anlaşılırken, varyans ayrıştırması testi de Bitcoin'in dışsal bir değişken olduğunu ortaya koymuştur. Son olarak yapılan granger nedensellik testi sonucunda ise Bitcoin'den Kanada Dolarına, İsviçre Frangına ve Çin Yuanı'na doğru tek yönlü bir nedensellik saptanırken diğer değişkenler arasında nedensellik ilişkisi bulunamıştır.

Anahtar Kelimeler: Kripto Para, Bitcoin, Blockchain, Döviz Kuru, Kriptoloji

ABSTRACT
MASTER THESİS

CRYPTO CURRENCY AND CRYPTOGRAPHİC TECHNOLOGY: ECONOMETRİC DATA ANALYSİS

TURGUT, Ecem
Department of Economics
Supervisor: Assoc. Prof. Okyay UÇAN
July 2020, 190 Pages

It has started to announce the name of crypto currencies with Bitcoin in the world economy. The popularity of Bitcoin, which was not known much at first, has increased in time and its transaction volume has reached more important dimensions. In addition, due to the high return rates of crypto currencies and very low transaction costs, different competitors such as Ethereum, Litecoin, Ripple, Dash, Neo, Monero have started to appear. Thus, these crypto currencies have an important place in the foreign exchange market. In this context, the relationship between crypto currency and exchange rate was analyzed in this context. In analysis, Bitcoin dependent variable; The most traded major currencies in the market such as Euro, British Pound, Australian Dollar, Japanese Yen, Canadian Dollar, Swiss Francs and Chinese Yuan are considered as independent variables. Variables covering the monthly data of period 2013-2019 were used and cross exchange rates against USD were used. ARDL analysis was performed to analyze the cointegration relationship and a long-term relationship could not be detected between the variables. Then VAR analysis was applied. As a result of the cusum test, it was understood that the variables were in a safe band range and The variance decomposition test revealed that Bitcoin is an external variable. A causality relationship was not found between other variables that found a one-way causality from Bitcoin to the Canadian Dollar, the Swiss Francs and the Chinese Yuan.

Keywords: Crypto Currency, Bitcoin, Blockchain, Exchange Rate, Cryptology

İÇİNDEKİLER

İKİNCİ BÖLÜM

KRİPTO PARA EKONOMİSİ: BİR BLOCKCHAİN UYGULAMA ALANI OLARAK BİTCOİN VE ALTCOİNLER

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA VE DÖVİZ KURU İLİŞKİSİ: UYGULAMALI ZAMAN SERİSİ ANALİZİ

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devletleri

ADF : Augmented Dickey Duller

AES : Advanced Encryption Standard

AIC : Akaike bilgi kriteri

ARDL : Autoregressive Distributed Lag Model

ASIC : Application Specific Integrated Circuit

AUD : Avustralya Doları

BC : Blockchain

BTC : Bitcoin

BTCEUR : Bitcoin Euro Endeksi

CAD : Kanada Doları

CHF : İsviçre Frankı

CPU : Central Processing Unit

CRIX : Kriptografik Para Endeksi

DAG : Directed Acyclic Graph

DAO : Decentralizet Autonomous Organization

DES : Data Encryption Standard

DF : Dickey Fuller

DH : Diffie-Hellman Asimetrik Şifreleme Algoritması

DLT : Distributed Ledger Tecknolohy

DOGE : Dogecoin

DSA : Digital Signature Algorithm

ECC : Eliptik Eğri Algoritması

EFT : Elektronik Fon Transferi

EKK : En Küçük Kareler Yöntemi

ETH : Ethereum

EUR : Euro

EURUSD : Euro ABD Doları Endeksi

GBP : İngiliz Sterlini

GPU : Graphichs Processing Unit

JPY : Japon Yeni

KKTC : Kuzey Kıbrıs Türk Cumhuriyeti

LPT : Sol Düz Metin

LTC : Litecoin

MB : Merkez Bankası

PoS : Proof of Stake

PoW : Proof of Work

PP : Philips-Perron Testi

P2P : Peer to Peer

RC2 : Rivest Cipher

RPOW : Yeniden Kullanılabilir İş İspatı

RPT : Sağ Düz Metin

RSA : Rivest-Shamir-Adleman Asimetrik Şifreleme Algoritması

SC : Schwartz bilgi kriteri

TDK : Türk Dil Kurumu

USDCNY : Çin Yuanı ABD Doları endeksi

USDT : Tether

VAR : Vektör Otoregresyon Modeli

XBTEUR : Bitcoin Euro Endeksi

XBTUSD **:** Bitcoin ABD Doları Endeksi

XBTCNY **:** Bitcoin Çin Yuanı Endeksi

XMR **:** Monero

XRP **:** Ripple

GİRİŞ

Kripto para birimleri ilk olarak 2008 yılının Ekim ayında Satoshi Nakamoto tarafından Bitcoin'in üretilmesiyle kendini göstermeye başlamıştır. Bu para birimleri kriptografik yöntemler kullanan, merkezi bir otoriteye bağlı olmadan eşler arası elektronik sisteme dayanan bir sanal para birimi şeklinde tanımlanmaktadır. Şifreli para birimlerinin bu şekilde bir kamu otoritesine bağlı olmadan yönetilmesi bu para birimlerinin maliyetinin çok düşük oranlarda gerçekleşmesine neden olmuş ve dolayısıyla hem gerçek kişiler hem de kurumsal yapılar tarafından büyük ilgi çekerek sanal piyasalarda kullanılmaya başlanmıştır.

Kripto para birimlerinin ilki ve en popüleri olan Bitcoin ise 2008 yılında isminin gerçek olup olmadığı hakkında şüpheler olan Satoshi Nakamoto'nun "Bitcoin: A Peer-to-Peer Electronic Cash System" adlı makaleyi yazmasıyla birlikte ortaya çıkmış ve dikkatleri üzerine çekmeyi başarmıştır. Daha sonraki süreçte ise Bitcoin piyasalarda ödeme aracı olarak kullanılmaya başlanmış ve bu işlem 2009 yılı içerisinde gerçekleşmiştir. Bitcoin'in zaman içerisinde ilgi çekmeye başlamasıyla birlikte Ethereum, Litecoin, Dash gibi farklı kripto para birimleri de ortaya çıkmaya başlamış ancak 2008 yılından bu yana Bitcoin popülaritesini asla kaybetmeyip en popüler kripto para birimi olarak piyasalarda varlığını korumuştur.

Kripto para birimlerinin bu kadar yakın bir zamanda kendini göstermeye başlamasından dolayı ise kripto paraların ne olduğu, türlerinin ne olduğu ya da ne işe yaradığı gibi teorik bilgilerin yetersizliğinin yanı sıra, bu para biriminin işleyişi, güvenliğinin nasıl sağlandığı, diğer ekonomik faktörlerle olan ilişkileri ve diğer para birimleriyle etkleşimleri yönünden de bilgi eksiklikleri bulunmaktadır. Bu bilgi eksiklikleri hem bireyler hem de ülkeler arasında yapılan e-ticaret işlemlerini tehlikeye atmaktadır. Bu amaçla kripto paralara yönelik bilgi eksikliklerinin giderilmesi böylelikle de hem bireyler hem de ülkeler arasında güvenli ticaretin gerçekleşmesi gerekmektedir.

Çalışmanın amacı bu doğrultuda kripto para kavramını ve çeşitlerini ayrıntılı bir şekilde açıklayıp ekonometrik analiz yöntemlerini kullanarak Bitcoin'in majör

para birimleriyle olan ilişkilerini ortaya koymaktır. Çalışmada aynı zamanda kripto para içerisinde önemli bir paya sahip olan ve kriptoloji olarak adlandırılan şifreleme ile bunun tekniklerini matematiksel yöntemlerle açıklayıp kripto parayla olan ilişkilerini ortaya çıkarmak amaçlanmaktadır. Böylelikle kripto paranın güvenliğinin nasıl sağlandığı yönünden sorular aydınlık kazanmış ve kripto paralara olan güven de artmış olacaktır. Aynı zamanda bu para birimlerine olan güvensizliğin ve bilgi eksikliğinin ortadan kalkmasıyla, insanlar Bitcoin gibi kripto para birimleriyle işlem yapmaktan kaçınmayacak ve bu para birimleri geleceğe yön vermiş olacaktır. Çalışmanın sonunda günümüzde önemi giderek artan, ancak hakkında çok fazla bilgiye sahip olunmayan kripto paralara ve bunların işleyişlerine açıklık getirilmiş ve hem matematik hem de ekonometri biliminden yararlanılarak analiz edilmiş ve konuya ışık tutulmuş olunacaktır.

Çalışmanın ilk bölümünde bu amaçla öncelikli olarak para kavramı, paranın fonksiyonları ve özelliklerinden bahsedilmiş ve arkasından kripto paranın ne olduğu ile ilgili genel bilgiler verilmiştir. Açıklamalar yapılırken farklı kavramsal tanımlamalara yer verilerek çalışmada farklılıklar yaratılmıştır. Ayrıca çalışmanın ilk bölümünde, kripto para ile ilgili olarak daha önceden yapılmış olan çalışmalardan farklı olarak, kripto paranın güvenliğinin sağlanmasında kullanılan ve işleyişinde önemli bir yere sahip olan, aynı zamanda herkesin bu para sistemini anlamasına büyük bir engel teşkil eden şifreleme sistemi de matematik biliminden yararlanılarak açıklık kazandırılmıştır. Bu amacı gerçekleştirmek için matematiksel kriptoloji yöntemleri ayrıntılı bir şekilde açıklanmıştır. Diğer yandan kripto paraların işleyişleri hakkında bilgi verilirken kripto paraların temelini oluşturan blockchain teknolojisi de ayrıntılı bir şekilde açıklanmıştır.

Çalışmanın ikinci bölümünde kripto paraların işletilmesinde ve üretilmesinde en önemli paya sahip olana madencilerden ve madencilik kavramından bahsedilmiştir. Daha sonra kripto para cüzdanları ve piyasada önemli yer tutmayı başarmış kripto para türleri açıklanmıştır. En son ise kripto para ekonomisi açıklanmıştır. Bu başlık altında kripto paraların vergilendirilmesi, ülkelerin bu konudaki yaklaşımları ve bu para birimlerinin işlem gördüğü borsalardan bahsedilmiştir. Ayrıca kripto paralarda arbitraj uygulamasının mümkün olup olmadığı da bu bölüm kapsamında açıklanmıştır.

Çalışmada son olarak birçok yazarın farklı görüşlerinden yararlanılarak literatürde bu yönde yapılmış çalışmalara yer verilmiş ve böylelikle konuya çalışmanın dışında verilen farklı bakış açılarından da bakılması sağlanmıştır. En son ise birçok kişi tarafından uygulanan ve iktisadi analizlere temel teşkil eden ekonometri biliminden de yararlanılarak kripto para ile Euro (EUR), İngiliz Sterlini (GBP), Avustralya Doları (AUD), Japon Yeni (JPY), Kanada Doları (CAD), İsviçre Frangı (CHF) ve Çin Yuanı (CNY) arasındaki ilişki ortaya koyulmaya çalışılmıştır. Bu doğrultuda Bitcoin ve döviz kuru ilişkisi analiz edilmiştir. Çünkü dünya ekonomilerinin işleyişinde döviz piyasaları büyük önem arz etmekte ve hem ülke içerisindeki ekonomik faaliyetlerin yürütülmesinde hem de ülkelerin dış ülkelerle olan ticaretlerinin yürütülmesinde temel teşkil etmektedir. Döviz piyasalarında öncü para birimleri olarak Dolar ya da Euro gibi para birimleri dikkat çekmekle birlikte son zamanlarda kripto para birimi olarak adlandırılan ve şifreleme sistemine dayanan Bitcoin, Ethereum, Litecoin gibi bir çok para birimi de ekonominin işleyişi açısından önem arz etmeye başlamıştır. Dolayısıyla ekonomik açıdan bu analiz gerekli görülmüş ve bu doğrultuda analiz kapsamı belirlenmiştir. Böylelikle kripto paranın hem şimdiki durumu hem de gelecekteki durumu ile ilgili tahminler yapılmış ve kripto paranın dünyada nasıl bir konuma geleceği konusunda yapılan tahminlere farklı bir bakış açısı kazandırılmıştır.

BİRİNCİ BÖLÜM

PARANIN DÖNÜŞÜMÜ VE KRİPTO PARA

Ekonomik birimler paranın piyasada olmadığı süreçlerde bir malın başka bir mal ile olan değiş tokuşuna dayanan ve takas ekonomisi denilen bir sistem aracılığıyla ticaretlerini gerçekleştirmişler ve bu doğrultuda ihtiyaçlarını karşılamaya çalışmışlardır. Ancak zaman içerisinde bu sistemde yaşanan aksaklıklar para olarak bilinen bir nesnenin ortaya çıkmasında etkili olmuştur. Bu doğrultuda tarih boyunca para çeşitli şekillerde piyasada kendini göstermiştir. Çalışmanın ilk bölümünü oluşturan bu bölümde ise öncelikli olarak bir nesnenin para olarak nitelendirilmesi için gereken özelliklere ve paranın fonksiyonlarına değinildikten sonra takas ekonomisinden başlayarak bugünlere kadar kullanılan farklı para türlerinden bahsedilmiştir. En son ise paranın son formu olan ve ortaya çıktığı 2009 yılından beri dikkatleri üzerine çekmeyi başaran kripto paralardan ve bu paraların altyapısını oluşturan blockchain teknolojisinden bahsedilmiştir. Ayrıca konunun daha net anlaşılabilmesi amacıyla kripto paraların temelini oluşturan ve bu para birimlerindeki güvenliğin sağlanmasında en önemli unsur olan matematiksel şifreleme yöntemi ayrıntılı bir şekilde açıklanmıştır.

1. 1. PARANIN TANIMLANMASI

Para geçmişten günümüze kadar sürekli değişim göstermiş ve literatürde, özellikle de ekonomik alanda, sosyal bir kavram olarak kendine önemli bir yer bulmuştur. Ancak paranın tanımı herkes tarafından farklı yapılmış ve bu yönde net bir sınır çizilememiştir. Bundan dolayı genel bir para tanımı yapabilmek amacıyla paranın sahip olduğu özelliklerinden ve fonksiyonlarından hareket edilerek en geniş yönlü tanım ortaya çıkarılmaya çalışılmıştır. Bu doğrultuda paranın tanımını "insanların para olarak kabul edebileceği her şey" şeklinde ifade eden John K. Galbraith'in tanımı en ünlü para tanımı olarak kabul edilmektedir. Ancak bu tanımın

çok genel olması nedeniyle literatürde para tanımlanırken paranın soyut ve somut anlamları ayrı ayrı dikkate alınmıştır. Paranın somut anlamının tanımlanmasında paranın değişim aracı olma özelliği dikkate alınırken, soyut anlamda hesap birimi ve değer saklama aracı olma özelliğinden yararlanılmıştır. Bu kapsamda iktisatçılar parayı en genel anlamıyla "Bir mal ve hizmetin satın alınmasıyla birlikte, bu mal ve hizmetlerin bedelinin karşı tarafa aktarılmasında ya da borçların geri ödenmesinde kullanılan genel kabul görmüş her şey" olarak tanımlanmışlardır (Öztürk ve Koç, 2006:209-210).

1. 2. PARANIN FONKSİYONLARI

Çalışmanın bu bölümünde paranın mübadele aracı, hesap birimi, değer saklama ve biriktirme aracı olma fonksiyonları açıklanmıştır.

1. 2. 1. Mübadele (Değişim) Aracı

Parayı bono ve tahvil gibi tüm diğer varlıklardan ayıran en önemli özelliği paranın değişim aracı olarak işlev görebilmesidir. Dolayısıyla bir paranın ekonomide önemli bir yere sahip olmasına neden olan birinci işlevi, mübadele aracı olma görevini üstlenmesidir. Geçmişte takas (trampa) ekonomisinde para doğrudan kullanılmadığı için bireylerin isteklerinin birbirleriyle eşleşmesi gerektiğinden dolayı "mal ve hizmetlerin değiştirilmesi sırasında harcanan zaman ve değer kaybı" olarak ifade edilen işlem maliyetlerininde yüksek olmasına neden olmuştur. Ancak zaman içerisinde paranın bir mübadele aracı olarak kullanılmaya başlanmasıyla birlikte mal ve hizmetlerin el değiştirmesinde harcanan zaman asgari düzeye indirilerek işlem maliyeti ortadan kalmış ve ekonomik etkinlikte artış sağlanmıştır. Dolayısıyla paranın mübadele aracı olma fonksiyonun en önemli özelliği olarak, işlem maliyetlerini azaltırken uzmanlaştırmayı kolaylaştırması buna paralel olarak da ekonomide etkinliği artırması gösterilmektedir (Yıldırım, 2014: 174).

1. 2. 2. Hesap Birimi

Ekonomide çok sayıda mal ve hizmet olduğundan dolayı bu mal ve hizmetlerin fiyatları, para birimi cinsinden ölçülmekte ve bu paranın "hesap birimi"

olma fonksiyonu olarak gösterilmektedir. İlkel zamanlarda, yani takas ekonomisinin geçerli olduğu dönemlerde, mal ve hizmetlerin satın alınması için sığır, çiçek, deniz kabuğu gibi herhangi bir nesne hesap birimi olarak kullanılmıştır. Dolayısıyla ekonomide iki mal olduğu varsayımı altında, bir malın diğer ikinci mal cinsinden değerinin bilinmesinin yeterli olacağı varsayımı hâkim olmuştur. Ancak normal şartlar altında piyasada sadece iki ürün olmadığı ve her malında farklı kalite düzeyleri olduğu için bu fiziksel nesnelerin standart bir ölçüsü bulunamamıştır. Bunun sonucunda sistemde meydana gelen aksaklıklar ile birlikte para sistemlerinde, soyut tek tip ölçü birimi bu fiziksel ölçü birimlerinin yerini almıştır. Bu tek tip ölçü birimi sayesinde ekonomide var olan mal ve hizmetlerin tamamının değişim aracı cinsinden ifade edilmesini sağlayan tek bir fiyat (Euro, Dolar…) yaratılarak malların değerlerinde netlik sağlanmıştır (Parasız, 1998: 3).

1. 2. 3. Değer Saklama ve Biriktirme Aracı

Paranın mal ve hizmetlerin satın alınmasında bir değişim aracı olarak kullanılabilmesi için aynı zamanda değerini muhafaza etme özelliğine de sahip olması gerekmektedir. Paranın bu fonksiyonu, gelirin elde edildiği andan harcandığı zamana kadar geçen süre içerisinde, satın alma gücünü koruması ve bu gücün elde sürekli olarak tutulması anlamına gelmektedir. En genel değer saklama aracı, para olarak kabul edilse bile tahvil ve hisse senedi gibi farklı türden değer varlıkları da muhafaza gücüne sahip olmaktadır. Ancak bu şekilde farklı türden değer saklama aracı olmasına rağmen paranın genel kabul görmesinin nedeni paranın yüksek bir likiditeye sahip olmasıdır. Likidite, ekonomide bir varlığın başka bir değişim aracına dönüştürülmesindeki kolaylığı ve hızlılığıdır. Yani bir nesne ne kadar hızlı dönüştürülebiliyorsa o kadar likiditesi yüksek demektir. Zaten finansal varlık taleplerini etkileyen en önemli faktör olarak likidite gösterilmektedir. Dolayısıyla bir varlığın likiditesi ne kadar yüksek ise o varlığa olan talepte o kadar yüksek olmaktadır. Bu özellikte parayı daha da önemli hale getirmektedir (Tiryaki, 2013: 117-118).

1. 3. PARANIN ÖZELLİKLERİ

Ekonomide bir varlığın para olarak tanımlanabilmesi ve paranın, en başta mübadele aracı fonksiyonu olmak üzere, tüm fonksiyonlarını yerine getirebilmesi için paranın bazı özelliklere sahip olması gerekmektedir. Paranın çeşitli özellikleri mevcut olmakla birlikte taşınabilirlik, dayanıklılık, bölünebilirlik gibi bazı temel özellikleri bulunmaktadır. Bu özellikler şu şekilde sıralanmaktadır (Yıldırım, Karaman ve Taşdemir, 2014: 605-606; Paya, 2013: 20; Kahraman, 2019: 6-8):

I. Homojenlik: Paranın kolay tanınmasında etkili olan birinci unsur maddenin her yerinin aynı değerde olmasıdır. Dolayısıyla paranın homojenlik özelliği parayı temsil eden tüm objelerin aynı maddi değeri temsil etmesidir. Homojenlik özelliği, diğer madenler ile kıyaslandığı zaman, en çok altın ve gümüş madenlerinde görülmektedir. Diğer yandan günümüzde arz edilen kağıt paralar da homojenlik özelliğini yansıtmakta hatta bunun için kağıt paralar; resimler ve madeni bantlar ile desteklenmektedir.

II. Taşınabilirlik: Farklı mal ve hizmetler yine farklı alan ve bölgelerde insanların tüketimine sunulmaktadır. Dolayısıyla paranın farklı ortamlarda gerçekleştirilen alışverişlerde kolaylık sağlayabilmesi için paranın kolay bir şekilde transfer edilebilmesi gerekmektedir. Aksi takdirde paranın yaygınlık kazanması mümkün olmamaktadır.

III. Dayanıklılık: Herhangi bir varlık bozuldukça değerini kaybedeceğinden dolayı paranın bozulmaz ve dayanıklı bir yapıda olması gerekmektedir. Aksi takdirde bir varlık para olarak nitelendirilememektedir.

IV. Bölünebilirlik: Ticarete konu olacak bir varlığın, malın değerini tam karşılayabilmesi için parçalara ayrılarak bölünebilmesi yani malların en küçük birimini dâhi karşılayabilecek nitelikte olması gerekmektedir.

V. Taklit Edilememe: Kolay taklit edilebilecek bir nesne değerini korumakta yetersiz olacağı için paranın bu unsuru oldukça önemlidir. Günümüzde de paraların taklit edilmesini engellemek amacıyla özel kâğıt, filigran ve metal şeritler kullanılmaktadır.

VI. Genel Kabul Görme: Bir paranın piyasada işlev görebilmesi için herkes tarafından kabul edilip genel bir ödeme aracı olarak tüm alışverişlerde kullanılabiliyor olması gerekmektedir.

VII. Kolayca Algılanabilme: İnsanların, ticaret sırasında bir paranın gerçek mi yoksa sahte mi olduğunu kolayca anlayabilmesi gerekmektedir.

1. 4. GEÇMİŞTEN GÜNÜMÜZE PARANIN EVRİMİ

Çalışmanın bu kısmında geçmişten bugünlere kadar paranın aldığı çeşitli şekillerden bahsedilmiştir. Bu doğrultuda takas ekonomisi, mal para, itibari para, çek ve elektronik para birimleri açıklanmıştır.

1. 4. 1. Takas (Trampa) Ekonomisi

Ekonomik birimler paranın piyasada var olmadığı süreçlerde, değiş-tokuş işlemleri gerçekleştirerek faaliyetlerini yürütmeye devam etmişlerdir. Bu doğrultuda insanlar da ihtiyaçlarını karşılamak için, bir mübadele aracı kullanmadan, mallarını doğrudan elden ele değiştirmişler ve bu suret ile ticaretlerini gerçekleştirmişlerdir. Bu şekilde gerçekleştirilen alışverişe ise takas ya da trampa sistemi adı verilmektedir. Takas ekonomisi koşullarında, ilke olarak insanlar mallarını değiş-tokuş ederek tüm ihtiyaçlarını karşılayabileceklerini düşünmüşler ancak zaman içerisinde sistemde bazı zorluklarla karşı karşıya kalmışlardır. Dolayısıyla da sistem etkin bir şekilde işleyememiştir. Bunun en önemli sebeplerinden biri, bireyler arasında takas işleminin gerçekleşebilmesi için iki tarafın da aynı yerde ve zamanda aynı ortamda bulunmasını gerekmektedir. Dolayısıyla bir ticaret ortağı bulmak büyük zaman ve çaba gerektirmekte bu durumda sistem içerisinde işlem maliyetini oldukça yükseltmektedir. Diğer yandan takasın gerçekleştirilebilmesi için ekonomide "isteklerin çifte beraberliği" olarak adlandırılan durumun gerçekleşmesi yani tarafların isteklerinin birbirleriyle uyuşması, uyuşsa bile aynı zamanda tarafların mallarını birbirlerine sunmaya hazır olması gerekmektedir. Bu durum ise ekonomide serbest ve sürdürülebilir ticareti engellemektedir (Aşar, 2016: 20-21).

Ancak takas ekonomisinin etkinliğini azaltan tek problemler bunlar değildir. Takas ekonomisinde mal ve hizmetlerin fiyatı, diğer mal ve hizmetler cinsinden

hesaplanmaktadır. Dolayısıyla en önemli problemlerden bir diğeri de A ve B gibi iki malın olduğu bir durumda C malı gibi üçüncü bir malın devreye girme ihtimalinin bulunmasıdır. Böyle bir ihtimalin gerçekleşmesi durumunda eşit bir takas işleminin gerçekleşebilmesi için her malın birden çok fiyatı olması gerekmektedir. Yani bir malın, kendisi hariç, ekonomide mevcut mal sayısı kadar fiyatı oluşmaktadır. Böyle bir durumda ekonomide var olan malların sayısı (N) olmak üzere, gereksinim duyulan mal sayısı aşağıdaki formülle hesaplanmaktadır (Paya, 2013: 17-18).

$$\frac{N\,(N-1)}{2} \qquad (1)$$

Bu durumda piyasada 1000 farklı mal olduğu varsayılırsa toplamda 1000.(1000-1)/2=499,500 adet farklı fiyat oluşmaktadır. Dolayısıyla fiyatların kendi içerisindeki özelliklerine göre farklı şekillerde belirlenmesi ve piyasada bu kadar çok fiyatla karşı karşıya kalınması işlemleri oldukça zorlaştırmaktadır. Takas ekonomisindeki bu güçlüklerden dolayı ticaret için yeni yöntemler düşünülmüş ve zaman içerisinde ödemeler sisteminde gelişmeler yaşanmıştır (Şıklar, 2004: 7).

1. 4. 2. Mal Para

Takas ekonomisinin ortaya çıkarttığı zorluklarla birlikte geliştirilen ödemeler sisteminin ilk aşaması, mal para üzerinden gerçekleştirilmiştir. Mal para sistemi ekonomik birimlerin tamamı tarafından değerli kabul edilen, paranın temel özelliklerini ve fonksiyonlarını taşıyan dolayısıyla bir değişim aracı olarak işlev gören bir metanın para olarak kullanıldığı sistem olarak ifade edilmektedir. Deniz kabuklarının yerini alan mal paraların en yaygın türlerini ise bugün hâlen mücevher olarak değerini koruyan altın ve gümüş oluşturmaktadır. Mal para olarak kullanılan varlıkların en önemli özelliği bu varlıkların kendiliğinden yüksek bir değere sahip olmasıdır. Ancak o dönemde mal paralara ilişkin bazı sorunlarla karşı karşıya kalınmıştır. Bu sorunlardan en büyüğü mal paranın bir yerden başka bir yere taşınması konusunda bazı zorluklar yaşanmıştır. Aynı zamanda değerli madenlerden elde edilen bu madeni paraların zaman içerisinde nominal değerleri ile madeni içerikleri arasında farklılıklar oluşmuş ve savaş gibi bazı olumsuz şartların hakim

olduğu dönemlerde paranın değerli maden içeriklerinin azaltılması sorunlarıyla karşı karşıya kalınmıştır. (Çağlarırmak Uslu vd., 2013: 8).

Piyasada bu şekilde aynı nominal değere sahip fakat malın içeriği farklı olan iki malla karşı karşıya kalınmıştır. Parasal bir ekonomide ise iki farklı paranın aynı anda var olduğu durum üzerine ilk incelemeyi yapan Gresham bu durumda nominal değeri eşit olsa bile tüketicilerin, maden içeriği yüksek ve değerli olan malları ellerinde tutacağını ve düşük değerli olanı harcama eğilimde bulunacağını ifade etmiştir. O dönemde de piyasada "kötü para iyi parayı kovmuş" yani gümüş değişim aracı olarak kullanılırken altın tasarruf aracı olarak elde tutulmuştur. İktisat biliminde bu şekilde kötü paranın iyi parayı kovması durumuna "Gresham Yasası" adı verilmektedir (Süslü ve Baydur, 2002: 96).

1. 4. 3. İtibari Para

II. Dünya Savaşını takip eden 1944 yılında, Bretton-Woods'da, ABD önderliğinde 44 farklı ülkenin katılımıyla "Birleşmiş Milletler Mali ve Finans Konferansı" düzenlenerek birçok ülkenin para birimi, Amerika dolarına endekslenirken ABD dolarının altına bağlı olarak devam etmesine karar verilmiştir. Dolayısıyla altına bağlı olan tek para birimi dolar olurken diğer para birimleri de dolara bağlı hale getirilmiştir. Ancak geçen süreç ile birlikte, 1971 yılında, doların altın karşılığının bulundurulması zorunluluğu da bertaraf edilmiştir. Buna paralel olarak ülkelerin dolaşımdaki paralarının altın karşılığının bulunması zorunluluğu da ortadan kaldırılmıştır. Bu şekilde mal olarak bir değeri bulunmamakla birlikte mal ve hizmetlerin satın alınmasında bir değer ifade eden, taklit edilemeyeceğine yönelik güven unsuru içeren ve merkezi otorite üzerine kurulmuş itibari paralar kendini göstermeye başlamıştır. İtibari paraların en önemli özelliği altın ve gümüş olarak bir karşılığının bulunmamasıdır. İtibari paralar, ülkenin vatandaşları tarafından da genel kabul görmüş bir para birimi olarak kendini göstermektedir. Kısacası literatürde itibari para "Devlet tarafından yasal ödeme aracı olarak basılan ve üzerinde ifade edilen nominal değere göre satın alma gücünü belirleyen kağıt banknot" şeklinde tanımlanmaktadır (Çarkacıoğlu, 2016: 4-5).

Takas ekonomisinden bu yana geliştirilen her ödeme sisteminde yaşandığı gibi kâğıt para sisteminde de bazı problemlerle karşı karşıya kalınmıştır. Bu noktada

kâğıt paraların çalınmasının oldukça kolay olması ve büyük miktarda paranın taşınmasında sorunlar yaşanması gibi bazı zorluklarla karşılaşılmış ve buna paralel olarak, bankalarda vadesiz mevduat hesapları bulunan kişilerin kullanabileceği, çek sistemi geliştirilmiştir.

1. 4. 4. Çek

İtibari paranın, büyük tutarlı ödemelerin gerçekleştirilmesi sırasında, transfer işlemlerinin çok maliyetli ve güç olması yeni ödeme sistemlerinin ortaya çıkmasına neden olmuştur. Bu doğrultuda itibari parayı çek sistemi takip etmiştir. Çek, muhatap bankaya ibraz edildikten sonra çekin üzerinde yazılı olan miktarın banka tarafından lehtar ve hamil olarak isimlendirilen karşı tarafa ödenmesini emreden kıymetli bir evrak olarak tanımlanmaktadır. Çek ile gerçekleştiren bir ödeme sistemi nakdi ödemelerden çok daha büyük bir hızla gerçekleştirilmekte ve kesinliği daha yüksek olmaktadır. Dolayısıyla mevduat sahibi bireyler, nakdi paranın çalınması ve kaybolması tehlikesinden uzak durmuş olmaktadır. Çekin sağladığı bir diğer avantaj ise kaydi para yaratmaya yardımcı olup bankaların likiditeyi devam ettirebilmelerinin maliyetini düşürmesidir. Bu avantajların yanı sıra çek, nakdi bir ödeme aracı olmamanın etkisiyle, ödemelerin nakde dönüştürülmesinde bazı zorluklara neden olmaktadır. Örneğin nakde dönüştürülmesi için bankaya gitme zorunluluğu çek ile yapılan işlemlerin maliyetini yükseltmektedir. Diğer yandan çek'in takas edilmesinin zaman alması, keşidecinin faizsiz kredi miktarı kadar ödüllendirilmesine, bu durumda ödeme sisteminin etkinliğinin ve güvenliğinin azalmasına neden olmaktadır (Kirdaban, 2005: 8-30).

1. 4. 5. Elektronik Para

Bilişim teknolojilerinde meydana gelen hızlı gelişmeler ile birlikte ödemeler sisteminin etkinliğinde artışlar meydana gelmeye başlamıştır. Özellikle son 20 yıl içerisinde modern elektronik ticarette önemli gelişmeler yaşanırken elektronik ödeme sistemleri de zaman içerisinde giderek daha fazla dikkat çekmiştir. Bu durum elektronik ödeme sistemlerinin daha derin ve geniş çaplı araştırılmasına ve e-para sisteminin de farklı bakış açılarıyla tanımlanmasına neden olmuştur. E-para sistemi en genel anlamıyla, online olsun ya da olmasın, her türlü alışverişlerde elektronik araçlar

vasıtasıyla değiş-tokuş yapılmasına olanak sağlayarak, ödeme işlemlerinin gerçekleştirildiği sistem olarak tanımlanmaktadır (Kabir, Saidin ve Ahmi, 2015: 113).

Elektronik ödeme sistemlerini genel olarak elektronik-nakit, ön ödemeli kart, kredi kartları, banka kartları ve elektronik kontroller oluşturmaktadır. Sistemde bu temel araçların yanı sıra birçok farklı e-ödeme seçenekleri yer almakta ve bu büyük avantajlara neden olmaktadır. Elektronik ödeme sistemindeki gelişmeler, kâğıt para basılması nedeniyle ortaya çıkan kâğıt maliyetini ve çek sisteminin neden olduğu zaman kaybını engelleyerek fon transferlerinin çok kısa bir süre zarfında gerçekleşmesinde etkili olmuştur. Aynı zamanda e-ödeme hizmetleri, müşterilerin banka hesaplarına ve işlemlerine uzaktan erişmelerine ve yönetmelerine olanak sağlamasının da etkisiyle özellikle yeni aracılar, online tüccarlar ve tüketiciler tarafından sıkça tercih edilmeye başlanmıştır (Kim vd., 2010: 85).

Ödemeler sisteminde, e-paralar her ne kadar piyasada etkin bir rol oynamış olsa da, gelişmeler devam ederek süreklilik göstermiştir. Elektronik sistemde yaşanan bu olumlu gelişmeleri son zamanlarda kripto paralar takip etmiş ve sıkça gündeme gelmeye başlamıştır. Halk tarafından kripto paralar ve elektronik paralar aynı para birimi gibi algılanmakla birlikte kripto paralar farklı işleyen bir ödeme sistemi olarak piyasada kendini göstermeye başlamıştır. Kripto paralar çalışmanın bundan sonraki kısmında ayrıntılı bir şekilde açıklanmıştır.

1. 5. KRİPTO (ŞİFRELİ) PARA BİRİMİ

Kripto para birimin tanımının yapılması çok kolay olmamakla birlikte kelimenin kökeni İngilizcede şifre anlamına gelen “Crypto” ve para birimi anlamına gelen “Currency” kelimelerinin bir araya getirilmesiyle şekillenmiştir. Currency (para birimi) terimi ise Latince’de dolaşımda anlamına gelen “Currens” kelimesinden türerken her iki kelimede de “kullanımda olan değer” anlamına işaret edilmektedir. Bu doğrultuda kripto para, işlemleri güvence altına alarak işlemlerin kontrolünü sağlayan, bu transfer işlemlerini doğrulamak için kriptografik şifreleme algoritmasını kullanan ve üçüncü kişiye bağlılığı ortadan kaldırarak eşler arası bir sisteme dayanan para birimi olarak bilinmektedir. Dolayısıyla kripto para biriminin ne olduğunun anlaşılabilmesi için şifreleme kavramının ne olduğunun da iyi bilmesi gerekmektedir. Bu bağlamda basit bir ifadeyle şifreleme, bilgiyi okunamayan bir formata

dönüştürerek sadece gizli bir anahtara sahip olan kişi tarafından çözülüp deşifre edilebildiği bir tekniktir. Yani kriptografi olarak bilinen şifreleme; bilginin, karşı tarafca okunmasının istenmediği durumlarda, anlaşılmayacak hale dönüştürülmesi işlemidir (Houben ve Snyers, 2018: 20).

Sanal para birimleri merkezi bir otoriteye bağlı olmamakla birlikte arkalarında merkez bankası veya bir devlet bulunmamaktadır. Dolayısıyla dağıtık bir yapıya sahip olup arz edilen ve sonraki süreçte arz edilecek toplam miktar önceden belirlenmiştir. Bu durum devletlerin para basmak suretiyle kendilerine gelir yaratma durumlarını ortadan kaldırmasına sebep olmuştur. Aynı zamanda faizlerin ve enflasyonların yükseltilmesi aracılığıyla bu tarz yüklerin halka mâl olmasının önüne geçmede de bir tür destek niteliği taşımaktadır. Tüm bu durumlarda kripto paraların ortaya çıkmasındaki ana sebepler olarak gösterilmektedir. Yani kripto paralar tasarlanırken merkezi otoriteyi ortadan kaldırmak temel amaç olarak gösterilmiştir (Güven ve Şahinöz: 2018: 31).

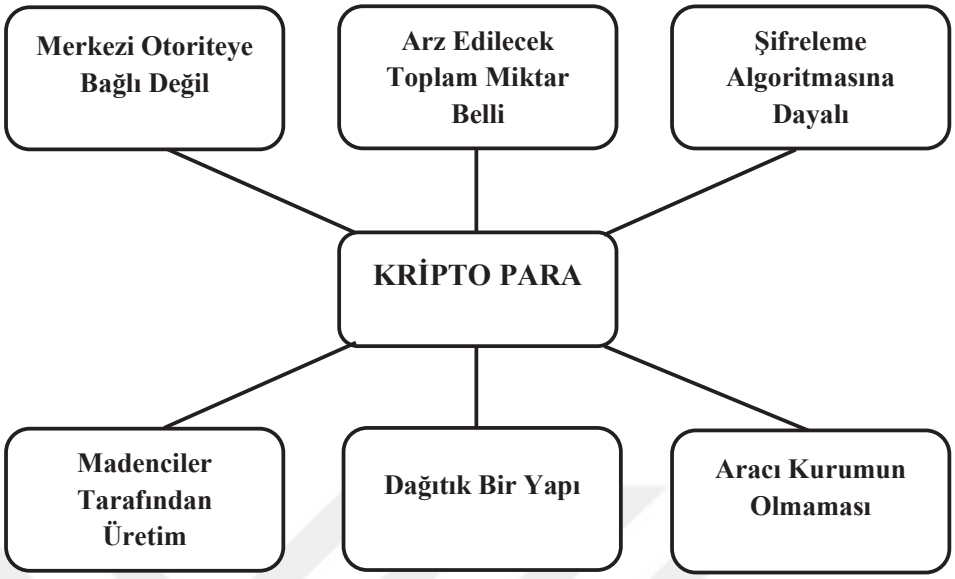
Kripto para birimleri özellikle son dönemlerde fazlasıyla ilgi çekmiş bir ödeme sistemi olup en önemli özelliklerinden biri Blockchain (Blokzincir) olarak bilinen bir dijital defter tutma sistemi üzerine kurulmasıdır. Temeli aslında 1980'li yıllara kadar dayanan kripto paralar, gerçek kimliği belli olmayan Satoshi Nakamato takma adlı bir kişi ya da kuruluşun 2008 yılında "*Bitcoin: A Peer-to-Peer Electronic Cash System"* isimli makaleyi yayınlamasıyla birlikte, dikkatleri çekmiş ve o günden beri giderek daha çok ilgi odağı haline gelmiştir. Bu sebepten Bitcoin adem-i merkeziyetçiliğe odaklanan ilk kripto para olarak bilinmekte ve kripto paranın öncüsü olarak tanımlanmaktadır. Bugün Litecoin, Ripple, Ethereum gibi 2500'ü aşkın kripto para birimi mevcut olmakla birlikte Bitcoin hâlâ en büyük piyasa kapitalizasyonuna sahip sanal para birimi olarak varlığını korumaktadır (Andrianto ve Diputra, 2017: 229).

1. 5. 1. Kripto Paranın Genel Özellikleri

Şifreli para birimleri uçtan uca bir ağ sistemine dayanırken herhangi bir merkezi otoriteye dayanmadan bağımsız olarak yönetilmekte ve madenciler (Mining, Miner) denilen bilgisayar kullanıcıları tarafından üretilmektedirler. Aynı zamanda sosyal dayanışmayı artırarak finansal aracıları ortadan kaldırma gibi özellikleriyle

geleneksel finansal sektörlere karşıt bir özellik sergilemektedir. Genel olarak finansal sistemin sağlıklı ve pürüzsüz bir şekilde işlemesi için içerisinde fon arz ve talep edenler, finansal araçlar, aracı kuruluşlar bulunması gerekmektedir. Finansal sistemler aynı zamanda yasal olmanın yanı sıra kurumsal düzenlemelerden de oluşmaktadır. Bu genel finansal sistem özelliklerinin herhangi birinde bir aksama meydan gelmesi sistemin işleyişinde bozulmalara neden olmaktadır. Bu noktada kripto paralar geleneksel sistemden ayrılmaktadır. Çünkü kripto paralarda merkezi bir otoritenin var olmayışı buna paralel olarak da kripto paralar üzerinde herhangi bir denetim mekanizmasının işlemeyişi finansal sistemin özelliklerine ters düşmektedir. Diğer yandan kripto paralarda aracı kurumların ortadan kaldırılması da bu duruma kanıt olarak gösterilmektedir (Adana Karaağaç ve Altınırmak, 2018: 126-127).

Sanal bir para birimi olarak piyasada kendine yer bulmuş olan kripto para birimleri, merkezi bir otoriteye özellikle de Merkez Bankasına (MB) bağlı olmadığından dolayı ülkelerin ekonomik durumlarından diğer para türlerine göre daha az oranda etkilenmektedir. Diğer yandan bu özellik piyasada kripto para talep edenlerin banka gibi merkezi bir otoriteye gitmeden işlem yapmalarına olanak sağlamıştır. Bu durum kripto para arz ve talep edenler arasında herhangi bir zaman kaybetmeden işlem yapılmasına neden olmuş ve işlem ücretlerini minumum noktaya çekmiştir. Şifreli para birimleri, dijital paralar ile açılmış hesapların dondurulması, el konulması gibi tehditleri ortadan kaldırmıştır. Kripto para birimlerinin nasıl işlediği konusunda ise değerlerinin, iktisatta temel kavram olan, arz ve talebe göre belirlenmesi ve değişim göstermesi kullanıcılara yol göstermektedir. Bu değerlendirme kapsamında kripto paralarda sonlu bir arz sisteminin mevcut olması yani arz edilecek toplam para miktarının, örneğin Blockchain platformunda üretilebilecek maksimum Bitcoin miktarının 21 milyon adetle sınırlandırılması gibi, önceden belirlenmesi sistemin nasıl işleyeceğine yönelik bilgi edinmeye ya da stratejik teoriler geliştirerek kazanç elde etmeye olanak sağlamaktadır (Çetiner, 2018: 2).



Kaynak: Yazar Tarafından Oluşturulmuştur.

Şekil 1: Kripto Paranın Genel Özellikleri

Kripto paranın genel özellikleri kapsamında en çok dikkat çeken unsur, bu sanal para birimlerinin nasıl üretildiği sorularını akla getirdiğinden dolayı, merkez bankasına ya da herhangi bir merkezi otoriteye bağlı olmamasıdır. Kripto paralar herhangi bir hükümete bağlı olmamakla birlikte üretimleri de varlıklarında olduğu gibi kullanıcı temelli bir modele dayanmaktadır. Üretilecek toplam miktarı en baştan belli olmasına karşın üretim işlemi madencilik (mining) şeklinde gerçekleştirilmektedir. Kripto para birimlerinde madencilik işlemi matematiksel şifreleme algoritmalarının çeşitli yazılımlar aracılığıyla çözülmesiyle gerçekleştirilmektedir. Dolayısıyla temel işlemci gücüne ve gerekli internet bağlantısına sahip olan herkes algoritmayı çözebilme ve kripto para üretme hakkına sahip olmaktadır (Azman, 2018: 62).

1. 5. 2. Kripto Para ve Elektronik Para birimi Ayrımı

Kripto para birimleri merkezi otoriteden bağımsız alternatif bir para birimi olup dijitaldirler. Bu dijitallik, merkez bankası gibi merkezi bir otorite tarafından ihraç edilen para karşılığında piyasa dolaşımı sağlanan ve karşılığı fiziksel para olan elektronik para ile kripto para birimlerinin birbirleriyle çok sık karıştırılmasına neden

olmuştur. Ancak elektronik para ve bu sanal paralar birbirlerinden tamamen farklı para birimlerini temsil etmektedir. Dolayısıyla bu noktada elektronik para ile kripto para ayrımının anlaşılması büyük önem taşımaktadır (Çetinkaya, 2018: 13).

Kripto paralar ve elektronik paralar temel olarak sayılar halinde mevcut olan, elle tutulamayan para birimleridir. Her iki para birimi de dijital para birimi olarak değerlendirilmekle birlikte elektronik paralar; banka havaleleri, banka ya da kredi kartlarıyla gerçekleştirilen ödeme sistemi olarak dolaşımdaki paraların büyük bir çoğunluğunu oluşturmaktadır. Ancak bir dijital para birimi olarak kripto paraların kendisi bir para birimidir. Yani tüm dijital para birimleri belirli bir kurum ve kuruluş tarafından düzenlenip belli bir otoriteye bağlıdırlar. Aynı zamanda merkezi olup her işlemleri saniye saniye ülkelerin merkez bankaları ya da devlet tarafından belirlenmiş kurumlar tarafından takip edilmektedirler. Dolayısıyla bu durum arkalarında yasal bir destek bulundurup dünya çapında geçerli olduğunu göstermektedir. Ancak kripto paralar diğer dijital para birimlerinden farklı olarak merkezi olmayan, düzensiz bir kurum ya da şifreleme topluluğu tarafından değerlerini belirleyen para birimleridir. Bu durum kripto paraların, elektronik paralardan farklı olarak, merkezi ya da hukuki olmadığını dolayısıyla dünya çapında geçerli olmayıp sadece belirli bir çevre tarafından kabul edildiğini göstermektedir (Nebil, 2018: 20).

Tablo 1: Sanal Para Birimleri ile Elektronik Para Birimlerinin Net Ayrımı

	Elektronik Para Birimi	**Kripto Para Birimi**
Konverte	Diğer para birimlerini temsil ederek konverte edilebilir.	Özgün bir sistem özelliği sergilediğinden sadece kendi birimince konverte edilebilir.
İhracı	Hükümetlerin kontrolü altındadır.	Bağımsız kişiler veya gruplar tarafından ihraç edilmektedir.
Arz Miktarı	Arz edilecek miktarda belirli bir sınırlama olmaksızın elektronik ortama aktarılan meblağ kadar olmaktadır.	Arz edilecek toplam miktar en baştan belli olmakla birlikte dönem içerisindeki arz miktarı sabit değildir..
Değer	İtibari değeri garantidir.	İtibari değeri garanti değildir.
Denetim	Hükümetlerin sürekli kontrolü altındadır.	Otoriteye bağlı olmadığından kontrol oldukça güçtür.
Riskler	Operasyonel risk	Operasyonel, hukuki, tedavül kabiliyeti gibi riskler

Kaynak: (Selçuk, 2019: 23).

1. 5. 3. Kripto Paranın Geleneksel Para Birimlerinden Farkı

Kripto para birimleri geleneksel para birimlerinden farklı bir yapıya sahiptirler. Dolar, Euro ya da TL gibi günlük yaşamda, her türlü işlem transferlerinde, alışverişlerde kullanılan geleneksel para birimleri merkezi otoriteye bağlı olup Merkez Bankası tarafından basımı yapılarak piyasaya sürülmektedir. Dolayısıyla piyasadaki arz miktarı ve bu para birimleri üzerinden yapılan işlemler Merkez Bankasının kontrolü ve denetimi altında olmaktadır. Ancak kripto paralar madenciler olarak bilinen bir grup tarafından üretilmekte olup herhangi bir merkezi otoritenin denetimi altında değillerdir. Diğer yandan geleneksel para birimleri devletin durumuna, ülke içerisindeki enflasyona, ticarete, krizlere, uygulanan politikalara ve buna benzer birçok ekonomik koşullara bağlıdırlar. Bu yüzden de kesin olarak hesaplanabilmektedirler. Ancak kripto para birimleri bağımsız olduklarından dolayı fiyat ve dalgalanmalarını belirlemek oldukça zordur. Bu farklılıklara karşın her iki para biriminde de fiyatların belirlenmesinde arz ve talep temel iki faktör olmaktadır (Andrianto ve Diputra, 2017: 229).

Bu noktada gizlilik açısından da geleneksel para birimleri ile kripto para birimleri birbirinden ayrılmaktadır. Geleneksel bankacılık sistemi, üçüncü kişilerin bilgilere erişimini sınırlandırarak gizlilik düzeyine ulaşmaktadır. Ancak bu noktada gerçekleştirilecek işlemlerin kamuya duyurulması zorunluluğunun bu yöntemin uygulanmasını önleyebilmekte fakat kripto paralardaki gibi genel anahtarları adsız tutarak da gizlilik korunabilmektedir. Dolayısıyla geleneksel para birimleri ile kripto para birimlerinin, gizliliği koruma açısından da birbirinden farklılıklar sergilediği anlaşılmaktadır. Bu bağlamda kripto para camiası da bu şifreli para birimlerini bölünebilirlik, taşınabilirlik, değiştirilebilir gibi temel para özellikleri açısından farklılık gösterdiğini belirtip geleneksel para birimlerinden üstün tutmuşlardır (Nakamoto, 2008: 6).

1. 5. 4. Kripto Paranın Para Olarak Değerlendirilmesi

Kripto para birimlerinin para olarak değerlendirilip değerlendirilemeyeceği sorunsalı sürekli gündeme gelmektedir. Bu yönden literatür incelendiğinde ekonomistler kripto paranın para olarak değerlendirilebileceğini savunanlar ve kripto paranın para olarak değerlendirilemeyeceğini savunanlar olmak üzere iki farklı gruba

ayrılmıştır. Ancak bu ikilemlere rağmen en doğru karar, çalışmanın başında da bahsedilen, paranın taşıması gereken özellikler ve paranın fonksiyonuna göre değerlendirilmesi ile verilecektir. Kripto paranın para olarak değerlendirilmesi ve bundan elde edilen sonuçlar Tablo 2'de gösterilmiştir.

Tablo 2: Kripto Paranın Para Olma Özelliği

Paranın Fonsiyonu	**Değerlendirme**	**Sonuç**
Değişim Aracı	Kripto paralar özellikle son zamanlarda daha da yaygınlık kazanarak tüketicilerin ilgisini çekmiş ve kullanım oranları sürekli artmıştır.	√
Değer Saklama Aracı	Yüksek volatilite oranlarına rağmen eskiyen, yıpranan ya da bozulan bir para birimi değildir.	√
Muhasebe Birimi	Resmi bir rapor henüz bulunmamasına rağmen uygulanmasına engel yoktur.	√
Paranın Özellikleri	**Değerlendirme**	**Sonuç**
Kabul Edilebilirlik	Kripto paralara yönelik güven her geçen gün biraz daha artmakta buna paralel olarak tanınırlığı ve kabul edilebilirliği de sürekli artmaktadır.	√
Değerinin İstikrarlı Olması	Kripto paraların en bilinir özelliği volatilitesinin yüksek olmasıdır. Yani kripto paraların fiyatlarında çok kısa sürede büyük dalgalanmalar gerçekleşebilmektedir. Bu para olarak değerlendirilmesinin önündeki en büyük engel olmaktadır.	×
Taşınabilir Olması	Piyasadaki hiçbir para birimi kripto paraların taşınabilirliği ve mobilitesi ile rekabet edebilecek kadar iyi bir seviyede değildir. Bu durum kripto paranın para olma yolundaki en önemli garantisi olarak gösterilmektedir.	√
Bölünebilirlik	Kripto paraların en iyi olduğu özelliklerden biridir. Örneğin bir Bitcoin 100 milyona bölünebilmektedir.	√
Ömürlü Olması	Piyasadaki banknotların aşırı yıpranması sonucunda Merkez Bankasının piyasadaki banknotları toplatıp piyasaya yenilerini sürmesi göz önünde bulundurulunca kripto paralar bu açıdan da para olma yolunda bir adım öne geçmeyi başarmaktadır.	√

Kaynak: (Güven ve Şahinöz, 2018: 38-39)

Tablo 2'den kripto paranın para olarak değerlendirilmesi için taşıması gerektiği özellikler ayrı ayrı değerlendirilmiş ve genel anlamda para olarak değerlendirilmesi için hiçbir engel olmadığı anlaşılmıştır. Bu yolda volatilitesinde sürekli ve anlık dalgalanmalar yaşanması engellenebilirse şifreli para birimlerinin para olarak değerlendirilmesinin önünde herhangi bir engel kalmayacak böylelikle tam anlamıyla herkes tarafından para olarak değerlendirilebilecektir. Ancak şuan mevcut olan durumda yukarıda da değinildiği üzere literatür bu yönde iki farklı gruba ayrılmaktadır.

Yermack (2013: 2-3)'de Bitcoin açısından konuyu ele almış ve Tablo 2'de varsayılanın aksine, kripto paraların iktisatçılar tarafından tanımlanan genel kriterlere göre para birimlerine uygun hareket etmediğini ancak internet stoklarına benzer spekülatif bir yatırıma benzediğini düşünmüştür. Ayrıca paranın özelikleri kapsamında kripto paranın bir değişim aracı olma özelliği taşımakla birlikte hesap birimi ve değer depolama aracı olarak düşük performansa sahip olduğunu ifade etmiştir. Bunlara ek olarak da Bitcoin; yaygın saldırı, hırsızlık ve diğer güvenlikle ilgili sorunlardan dolayı büyük zorluklarla karşı karşıya olurken ABD doları, Euro, Yen, İsviçre Frangı veya İngiliz Sterlini gibi diğer belirgin para birimleri ile ve aynı zamanda altın karşısında olduğu gibi döviz kurları ile de neredeyse sıfır bir korelasyon gösterdiği ve tüm bunların para olma önündeki en büyük engel olduğunu dile getirmiştir.

1. 5. 5. Kripto Paranın Avantajları ve Dezavantajları

Şifreli para birimleri, adem-i merkeziyetçi bir sisteme sahip olup blokzincir sistemine bağlı olarak bölünebilmektedirler. Bu sistemde, işlemler isimsiz olup herkes tarafından kontrol edilebilirken hiç kimsenin üzerinde herhangi bir güç yetkisi bulunmamaktadır. Diğer yandan merkezi sistemlerde, genellikle para birimleri üzerinde yönetim yetkisine sahip olan bir grup bulunmakta ve bunlar mevcut para biriminin başarısını garanti etmektedirler. Para birimini kontrol ederek de paranın kötüye kullanımını durdurmaya çalışmaktadırlar. Her iki siteminde kendi içerisinde bazı avantajları ve dezavantajları bulunmaktadır. Ancak kripto paralardaki belirsizliklerden ve piyasada yeni kendisini gösterip alışılmışın dışında özellikler

sergilediğinden dolayı bu sanal para biriminin avantajları ve dezavantajlarının açıklanması önem taşımaktadır (Milutinovic, 2018: 112).

Drozd, Lazur ve Serbin (2017: 222)'de kripto paraların avantajlarını şu şekilde sıralamıştır:

- Özellikle mikro iletilerde düşük işlem maliyeti
- Farklı kullanıcılar ve ülkeler arasında nispi para akış oranı
- Eş zamanlı güvenlik sistemiyle kullanıcılar için basitlik ve esneklik
- Fonlara el koymanın imkânsızlığı
- Bankacılık sisteminde yapılan sermaye hareketlerinden bağımsızlık
- Daha az bürokratik engeller

Literatür bu yönde Drozd, Lazur ve Serbin'in görüşlerini desteklerken kripto paranın avantajlarının sadece bu kadarla sınırlı olmadığı ancak bu konuda net bir bilgi eksikliğinin olduğu bilinmektedir. Bu noktada Bunjaku, Gorgieva-Trajkovska ve Miteva-Kacarski (2017: 37-38) konuyu ayrıntılı bir şekilde ele almış kripto paranın avantajlarına aşağıdaki maddeleri de ekleyerek ayrıntılı bir şekilde açıklamıştır.

- Madencilik kripto para birimi için açık kod (BTC) sağlamaktadır. Çevrimiçi bankacılıkta kullanılan aynı algoritmaları uygulamasına karşın aralarında bir fark bulunmaktadır. Bu da internet bankacılığında kullanıcılar hakkındaki bilgiler ifşa edelirken; BTC ağında işlemle ilgili tüm bilgiler paylaşılsa dahi alıcılar veya madeni paraların göndereni hakkında hiçbir veri bulunmamaktadır.
- Enflasyon riski ya da enflasyonun gelişme ihtimali yoktur. Çünkü arz edilecek toplam miktar önceden belirlendiği için ne siyasi güçler ne de düzeni değiştirecek şirketler bulunmaktadır.
- Eşler arası şifreleme para birimi ağına dayanmaktadır. Bu tür ağlarda tüm işlemlerden sorumlu ana sunucu yoktur. Bilgi alışverişi 2-3 ya da daha fazla yazılım müşterisi arasında gerçekleşmektedir.
- Sınırsız işlem imkânı sunmaktadır. Cüzdan sahiplerinin her birine, her yerde ve herhangi bir miktarda ödeme yapılabilmektedir. Böylece cüzdana sahip

başka bir kullanıcının bulunduğu herhangi bir yere transfer yapılmasına olanak sağlamaktadır.

- Sınır yoktur. Yani bu sistemde yapılan ödemeleri iptal etmek mümkün değildir. Sahte olamazlar, kopyalanamaz ve iki kez harcanamazlar.
- Düşük işlem maliyeti vardır. Çünkü bankalara ve diğer kuruluşlara komisyon ve ücret ödemeye gerek yoktur.
- Ağın bir kısmı çevrimiçi olmasa bile, ödeme sistemi aksamadan çalışmaya devam etmektedir.
- Kullanım açısından oldukça kolaylık sağlamaktadır. İşlem hızı ise oldukça yüksektir. Örneğin bir BTC cüzdanı oluşturmak yaklaşık 5 dakika gibi kısa bir süre almaktadır.
- Anonim bir özellik sergilemektedirler. Yani herhangi bir referansa ihtiyaç duymadan sonsuz sayıda kripto para adresi oluşturulabilmektedir.
- Şeffaflık en önemli özelliklerinden birini oluşturmaktadır. Blokzincir özelliği sayesinde gerçekleşen işlemlerin geçmişi tutulabilirken her türlü bilgi de saklanabilmektedir.
- Hesabın sadece sahibine ait olduğu eşsiz bir elektronik ödeme sistemine sahiptirler.
- Kişisel verileri kullanma şansı olmadığından dolandırıcılık riski neredeyse hiç yoktur.
- Şeffaf ve kârlı bir kaynağa fon yatırım imkânı sağlamaktadırlar.

Literatürde ele alınan tüm bu avantajlar karşısında kripto para talep edenler, bu kadar yeni bir para birimi olmasına rağmen, çok sayıda avantajı varken dezavantajlarının da fazla olabileceği şüphesi içerisine girmektedir. Bu bağlamda şifreli para birimi özelliğine sahip olduğu bilinen ilk başarılı kripto para birimi olarak Bitcoin'in bile hâlâ olgunlaşma aşamasında olduğu bilinmektedir. Geliştiriciler ise bu yönde Bitcoin'in kırılganlığını ve dezavantajlarını azaltmak için sürekli çaba sarf etmektedirler (Vyas ve Lunagaria, 2014: 12).

Bondarenko, Kichuk ve Antonoc (2009: 12)'de kripto paranın dezavantajlarını birkaç madde ile açıklamışlardır. Buradan çıkan sonuç doğrultusunda kripto paranın dezavantajları aşağıda verilmiştir:

- İnternete yönelik para biriminin hareketlerini izlenmenin ve denetlemenin imkânsız olması.
- Gerçekleştirilen bir ödeme işleminin geri çekilmesinin ya da iptal edilmesinin imkânsız olması.
- Depolama ve para transfer işlemlerinde hâlâ bazı şüphelerin bulunması.
- Kripto para borsalarındaki hesabın çalınması ve ele geçirilmesi gibi güvenlik sorunlarının sürekli duyulması kripto para talep edenleri tedirgin etmektedir. Bu durum sanal paraların yaygınlık kazanmasına engel olmaktadır.
- Bu sanal para birimlerinin, geleneksel para birimleriyle takası da bir tür sorun oluşturmaktadır.
- Yüksek volatilite oranları. Kripto paralar kısa sürede, hükümetlerin beyanlarına bağlı olarak, sürekli inişler çıkışlar göstermektedir. Kripto paranın en büyük dezavantajı ve para olarak değerlendirilmesinin önündeki en büyük engelde bu özellikten kaynaklanmaktadır.

Bu dezavantajlara rağmen, literatür ayrıntılı bir şekilde incelendiği zaman, bilim dünyasında kripto para birimlerinin geleceğinin çok parlak olduğu ve sağladığı bu avantajların, dezavantajlarını gölgede bırakacağına yönelik yaygın bir görüş hakim olmaktadır. Komisyoncuların aradan çıkarak işlem maliyetlerinin azalması ve özellikle de uzak mesafelerden kaynaklı ticaret engellerini ortadan kaldırmasının etkisiyle ülke ekonomileri açısından olumlu yönde gelişmeler yaşanacağı gibi beklentiler içerisinde olunduğunun da bu noktada belirtilmesi gerekmektedir (Bunjaku, Gorgieva-Trajkovska ve Miteva-Kacarski, 2017: 38).

1. 5. 6. Kripto Paranın Öncüleri

2008 yılında Satoshi Nakamoto adını kullanan kimliği belirsiz bir programcının dijital para birimlerini açıklayan bir makale yayınlayıp bundan bir yıl sonra da Bitcoin ağını başlatmasıyla birlikte, 3 Ocak 2009 tarihinde, ilk Bitcoin işlemini gerçekleştirilmiş ve kripto paralar piyasada kendilerine yer bulmaya

başlamışlardır. Ancak bu durum kripto para fikrinin bir anda mı orta çıktığı, Bitcoin'den önce merkezi bir otoriteye ya da bankaya ihtiyaç duyulmayan şifreli bir para fikrinin başkaları tarafından ortaya atılıp atılmadığı ya da Nakamoto'nun bu yolda tek mi olduğu gibi bazı soruların düşünülmesine neden olmuştur. Bu noktada soruların açıklık kazanması için Bitcoin öncesi kripto para girişimlerine ya da düşüncelerine çalışma kapsamında yer verilip aydınlık kazandırılması önem kazanmaktadır (Rose, 2015: 618).

Bu bağlamda, dijital para endüstrimanlarının özel kategorilerinde bile, bazı araçların Bitcoin'den önce var olduğu bilinmektedir. Bunlar Bitcoin'in sonrasında merkezi ya da önde gelen bir pozisyonda yer almamıştır. Ancak Bitcoin'e benzer özellikler taşıyan başka dijital parasal araçlar olarak varlığını göstermişlerdir. Bunun en önemli örneği David Chaum ve Stefan Brands'in coin üretme tabanlı eCash'i geliştirmesi olmuştur. Adam Back ise HashCash olarak bilinen spam kontrolü için bir iş ispatı programı hazırlamıştır. Daha sonraki süreçte ise Hal Finney tarafından HashCash'teki algoritma tekrar kullanılarak bir yeniden kullanılabilir iş ispatı (RPOW) geliştirilmiştir. Diğer yandan Wei Dai'nin B-Money'si ve Nick Szabo'nun Bit-Gold'unu içeren dijital boyutlu dağılmış olan kripto paralar için yenilikçi öneriler yapılmıştır. Bu yenilikçilerin temelini atan Bitcoin ise Satoshi Nakamoto isimli kimliği tam olarak belli olmayan bir kişi ya da kuruluş tarafından ortaya çıkarılmıştır. Tüm bu bağlantıların bir araya getirilmesi sonucunda Wei Dai ve Hal Finney'in Nakamoto'nun ajanı ya da temsilcisi olduklarından şüphe duyulmuştur. Ancak bu iddiaları kendileri reddetmişlerdir (Chohan, 2017: 1-2). Kripto paranın öncüleri Tablo 3'de gösterilmiştir.

Tablo 3: Kripto Paranın Öncüleri

Nick Szabo	1983 yılındaki bir makalesiyle birlikte kripto para fikrinde bir takım kıpırdanmalara neden olmuş ve 1990'lı yıllarda birçok kişinin kripto para konusuna ilgi göstemesine öncülük yapmıştır. Aynı zamanda Bitcoin'in ilk habercisi olarak bilinen dijital para mekanizmasını geliştiren bilgisayar bilimcisidir.
Tim C. May	CyberPunk Mail listesini kuran kişidir.
David Chaum	eCash protokollerini kurmakla birlikte DigiCash'i de kurmuştur.
Stefan Brands	David Chaum ile birlikte eCash protokolünü geliştirmiş ve dolayısıyla Brands de DigiCash'ın kurucusu olmuştur.
Hal Finney	PGP Corporation kurusucu olarak bilinmekle birlikte Hal Finney'in kripto para piyasasında, Satoshi Nakamoto tarafından ilk Bitcoin transferinin yapıldığı bu doğrultuda da işlem onayını geliştirmiş kişi olarak dikkatleri üzerine çekmiştir. Ancak Nakamoto ile olan bu tranfer alışverişlerine rağmen Finney bir mesajında gerçekten Nakamoto'yu tanımayıp, kim olduğunu bilmediğini açıklamıştır.
Adam Back	HascCash'i geliştiren kişi olarak bilinip literatürde Satoshi Nakamoto ile ilk temas edenler biri olarak tanıtılmaktadır.
Wei Dai	B- Money'in kurucusu ve Adam Back'ten sonra Nakamoto ile temas kuran ikinci kişi olarak bilinmektedir.
Phil Zimmerman	PGP Encryption

Kaynak: (Nebil, 2018: 22-23).

1. 5. 7. Kripto Para Tarihindeki Önemli Olaylar

Satoshi Nakamoto'nun 2008 yılında Bitcoin üzerine bir makale yayınlamasıyla birlikte kripto para piyasaları ilgi çekmeye başlamıştır. Dolayısıyla piyasadaki şirketler veya hanehalkları tarafından sürekli incelen bir para birimi haline gelmiş, herkes kripto para gündemini dikkatle incelemeye başlamıştır. Ancak bu para biriminin bu kadar yeni olmasının da etkisiyle gündeme, bazı dönemlerde olumlu bazı dönemlerde olumsuz yönleriyle, gelmiştir. Dolayısıyla çalışma kapsamında gerçekleşen bu olaylara kısaca açıklık kazandırılması kripto paraların nasıl bir eğilim gösterdiği ve gelecekte nasıl bir gelişme gösterip piyasada kendisine nasıl yer bulacağının anlaşılması yönünden önem kazanmaktadır. Bu noktada konu üzerine gündemde yaşanan en önemli olaylar Tablo 4'de gösterilmiştir. Bu noktada verilen olayların dışında daha birçok olayında gündeme geldiğinin bilinmesi gerekmektedir.

Tablo 4: Şifreli Para Birimlerinde Öne Çıkan Olaylar

Tarih	Gerçekleşen Olay
31 Ekim 2008	Satoshi Nakamoto tarafından bir makale yayınlanmıştır. Makalede Bitcoin'in tasarımı ve nasıl çalıştığıyla ilgili ayrıntılı bilgiler verilmektedir.
3 Ocak 2009	İlk blok olan Genesis Bloğu çıkartılmış böylelikle Bitcoin Madenciliği başlamıştır.
9 Ocak 2009	Bitcoin'in 0.1 sürümü yayınlanmıştır.
12 Ocak 2009	İlk Bitcoin transfer işlemi, Nakamoto ve Hal Finney arasında gerçekleştirilmiştir.
5 Ekim 2009	New Liberty Standard, ilk Bitcoin değerini hesaplamış ve böylelikle ilk kez Bitcoin kuru oluşturulmuştur. Ayrıca ilk Bitcoin alışveriş fiyatları yayınlanmıştır.
16 Aralık 2009	Bitcoin 0.2. sürümü yayınlanmıştır.
30 Aralık 2009	Bitcoin'in zorluk derecesi ilk kez artmıştır.
22 Mayıs 2010	Laszlo Hanyecz tarafından, Bitcoin kullanılarak yapılan ilk alışveriş gerçekleştirilip 2 pizza karşılığında 10.000 Bitcoin ödenmiştir. Kripto para tarihinde bu olay "pizza Day" olarak bilinmektedir.
7 Haziran 2010	Bitcoin'in 0.3 sürümü yayınlanmıştır.
18 Temmuz 2010	OpenGL GPU has çiftliği kurulup ilk Bitcoin bloğu üretilmiştir.
18 Ekim 2010	İlk madencilik havuzu açılmıştır.
12 Haziran 2011	İlk büyük balon etkisi yaşanmıştır.
6 Eylül 2011	Casascius Coins, ilk fiziki Bitcoin'i basmış ve böylelikle metal paraların içerisine Bitcoin'de yerleştirilmiştir.
19 Şubat 2013	Bitcoin'in 0.8 sürümü yayınlanmıştır.
2 Mayıs 2013	İlk Bitcoin ATM'si California'da kurulmuştur.
…Temmuz 2013	İlk Türk Bitcoin borsası olan BTCTurk açılmıştır.
21 Kasım 2013	University of Nicosia ödemelerde Bitcoin'i kabul eden ilk üniversite olmuştur.
… Ocak 2014	Bir e-ticaret devi olan Overstock ödemelerde Bitcoin kabulüne başlamıştır.

25 Şubat 2014	Mt.Gox sitesinden Bitcoin çalındığı haberleri gündeme gelmiştir. Bunun üzerine 1 Mart 2014'de Mt.Gox iflas ettiğini açıklamıştır.
23 Mart 2014	Kripto para üzerine türkçe yayın yapan Coin-Turk.com hizmete girmiştir.
11 Şubat 2015	CAVIRTEX, güvenlik sorunları ile kapatılan borsa siteleri arasına girmiştir.
16 Kasım 2015	Ekonomi profesörü olan Bhangwan Chowdhry, Nobel Ekonomi ödülüne Satoshi Nakamoto'yu gösterdiğini Twitter üzerinden açıklamıştır.
6 Mayıs 2016	"Bitstamp" Avrupanın ilk lisanslı Bitcoin borsası olmuştur.
12 Mayıs 2016	Bir kripto para birimi olarak Coinbase ve Ripple'ın lisans alacağı duyurulmuştur.
9 Temmuz 2016	Bitcoin ağına yeni bir blok eklendiği zamanlarda, bloğu ekleyen madenciye ödül olarak piyasaya yeni girecek Bitcoin'ler verilmektedir. İlk başta bu ödül 50 BTC iken, tarihi tam belli olmamakla birlikte, 2012 yılında 25'e düşürülmüştür. Daha sonra 9 temmuz 2016 yılında bu rakam 12.5 BTC'e düşürülmüş ve bu olay literatüre Halving Day olarak geçmiştir.
5 Nisan 2017	Bitcoin'in blok boyutundaki sorunlara çözüm getireceği düşünülen "SegWit" uygulamasının "Litecoin" üzerinde deneneceği açıklanmıştır.
25 Nisan 2017	IMF, Blockchain için ilk kez toplanmıştır.
25 Mayıs 2017	Japonya'da kripto para adına önemli bir adım olan Bitcoin mevduat hesabı açılmıştır.
12 Haziran 2017	Nevada, Blockchain vergisini kaldıran ilk eyalet olarak tarihe geçmiştir.
18 Haziran 2017	Apple kurucusu Steve Wozniak'da Bitcoin'e yatırım yapacağını açıklamıştır.
29 Haziran 2017	Dünya Ekonomik Forumu, Blockchain raporu yayınlamıştır.
1 Ağustos 2017	"Bitcoin Cash" doğmuştur.
4 Kasım 2017	TCMB, kripto paraların finansal istikrarı sağlayabileceği yönünden görüşlerini bildirip kripto paralara olan güvenin birazda olsa artmasına neden olmuştur.

Kaynak: (Kurt, 2018: 26-41; Nebil, 2018: 33-37).

1. 6. BLOCKCHAİN VE ŞİFRELEME TEKNOLOJİSİ

Kripto para piyasalarına yatırım yapılmasının önündeki en büyük engellerden biri herhangi bir devletin ya da kurumun kontrolü altında olmamasına rağmen güvenliğin nasıl sağlandığının net olarak anlaşılamamasıdır. Kripto paralarda güvenlik iki bölümden oluşmaktadır. İlk bölümünü madenciler tarafından "sıkışık Hash kesişimleri" bulmak oluştururken ikinci bölümünü "%51 atağı" olarak bilinen sistem oluşturmaktadır. İkinci yapıda, ağın %51'inden daha fazla kazı gücüne sahip olan madenciler, küresel blokzincir sistemine müdahale edip değiştirerek, alternatif bir ana defter yaratmaktadırlar. Çalışmanın bu kısmında güvenlik açısından önemli bir nokta olan bu blockchain (BC) teknolojisinden ve altından yatan şifreleme algoritmasından ayrıntılı bir şekilde bahsedilmiştir (Azman, 2018: 61).

Öncelikli olarak blockchain, çok sayıda düğüm içerisinde tutarlı olan işlemlere karşı dayanaklı bir işlem veritabanıdır. Geriye dönük manipülasyona karşı veri depolamasında kriptografik güvence sağlarken yeni işlemlerin doğrulanması gerektiğinde, veritabanında tutarlılığı sağlamak için bir fikir birliği mekanizmasını kullanmaktadır. Dolayısıyla blokchain teknolojisinin anlaşılmasında veri ve veri tabanının ne olduğunun da iyi bilinmesi gerekmektedir. Bu noktada konu ayrıntılı bir şekilde anlatılmadan önce bu kısmın kavramsal olarak aydınlatılması konunun anlaşılması açısından fayda sağlayacaktır (Beck, 2018: 55).

Veri; bir bilginin ham parçasıdır. Sadece ölçüm, sayım deney ve gözlem yöntemleriyle değil aynı zamanda araştırma yoluyla da veri elde edilebilmektedir. Burada önemli olan nokta, verilerin işlenmesi ve matematiksel süreçler geçirilmesi gerektiğinden dolayı, tek başlarına herhangi bir anlam ifade etmemesidir. Ancak veriler işlendikten sonra bir takım bilgi haline gelmektedirler. Bu şekilde de çeşitli problemlerin çözülmesindeki önemli bir unsuru oluşturmaktadırlar. Dünyada hesaplanmayacak boyutta bir veri depolaması mevcuttur. Ancak bu sayısız verinin, bilgisayar ortamındaki depolama işlemi gerçekleştirilirken veritabanı ihtiyacı ortaya çıkmaktadır. Veri tabanı ise; verinin düzenli bir şekilde listelenmesini sağlayarak veriye ulaşmayı kolaylaştıran bir nevi koleksiyon yapısıdır (Gündüz ve Tepeci, 2018: 39-40).

1. 6. 1. Blockhain Teknolojisi Nedir?

Türkçe karşılığı blokzincir olarak ifade edilen bu teknoloji, temelde dağıtılmış bir veri tabanı sistemine dayanarak, katılan taraflar arasında gerçekleştirilen ve paylaşılan tüm işlemlerin ya da dijital olayların halka açık defteri olarak tanımlanmaktadır. Blokzincirin bu kadar gündeme gelmesindeki en önemli potansiyeli bu işlemlerin ya da verilerin kaydedilişine yönelik kullandığı teknolojiden kaynaklanmaktadır. Halka açık defterlerdeki her işlem sistemdeki katılımcıların çoğunluğunun oy birliğiyle doğrulanmaktadır. Burada en önemli nokta, sisteme girilen hiçbir bilgi silinememekte ve şifreli olan bir veriyi zincir halka gibi birbirine bağlayarak değiştirilmez bloklar halinde birleştirilmektedir. Yani blockchain'de sistem daha önceden mevcut olan bir bloğun arkasına veriler bloklar halinde kaydedilmekte ve bir blok dolduğu zaman sonraki blok üretilmektedir. Bilgilerin silinip değiştirilmemesinin arkasında yatan sebepte bundan kaynaklanmaktadır. Çünkü bir bloğun silinip değiştirilmesi için diğer tüm bloklarında değiştirilmesi gerekmektedir. (Crosby vd., 2016: 8).

Kripto paralarda bu açıdan önemli olan nokta işlem yapacak kişilerin blokzincirde kaydedilen hiçbir bilginin ya da işlemin değiştirilmeyeceğini bilerek, özellikle teknoloji içerisinde para gönderme işlemi gerçekleştirileceği zaman, gönderilen kişiden, birim ve adresten emin olarak işlemlerini onaylamaları gerekmektedir. Çünkü sistemde işlem gerçekleştikten sonra mühürlenmektedir. Dolayısıyla geri dönüşü kesinlikle mümkün olmamaktadır (Atabaş, 2018: 12).

1. 6. 2. Blockchain Kullanım Alanları

Kripto paraların önemli teknolojisi olan blokzincir, para transferleri ve bankacılık gibi işlemlerin gerçekleştirilmesi için büyük bir verimlilik ve güvenlik sağlamaktadır. Özellikle, Bitcoin savunucuları her ne kadar BC sisteminin klasik bankacılık sektörünün sonunu getireceğine inansalar da, blokzincir teknolojisine en hızlı adapte olmayı başaran sektörlerden biri bankacılık olmuştur. Örneğin dünyanın en büyük bankaları arasında yer alan "Barclays" operasyon maliyetlerini düşürmek için BC teknolojisini kullanmıştır. Ancak BC'nin kullanım alanı sadece bununla sınırlı kalmamaktadır. Blokchain teknolojisinde kaydedilen tüm veriler veya bilgiler; para transferleri, işlemlerin düzeni, işlemi gerçekleştiren kişilerin kimliğinin

gerçekleştirilmesi, sözleşme onayı gibi birçok işlemi hesaplayacak şekilde tasarlanmıştır. Bundan dolayı blokzincir sadece kripto paralara özgü bir sistem olarak algılanmaması gerekmektedir çünkü hayatın her alanında kullanılabilecek bir sistem yapısı sergilemektedir (Aksoy, 2018: 32-33).

Özcan (2019: 6-7)'de bu noktaya aydınlık kazandırmak amacıyla BC sisteminin çeşitli kullanım alanlarını ve amaçlarından bazılarını şu şekilde sıralamıştır:

I. Uçtan uca para gönderme: Adem-i merkeziyetçi bir yapıda düşük masraflı, hızlı ve şeffaf ödeme altyapısı hazırlayarak para transferini olanaklı hale getirmektedir. Sistem içerisindeki cüzdanlar (Wallet) aracılığıyla da bu bakiyelerin takip edilmesi güvenli hale gelmektedir.

II. Dijital kimlik: Dijital kimlikler merkezi bir otorite tarafından korunsa bile verilerin çalınıp manipüle edilme olasılığı oldukça yüksektir. Dolayısıyla kimliklerin bir blokzincir yapısında kullanılıp tasarlanması daha esnek ve doğru tanımlama yapısının korunmasına olanak sağlayacaktır. Kurumların kendi veri tabanları tutması da zaman ve para kaybetmeyi önlemiş olacaktır.

III. Oylama sistemi: Güney Koreli bir kripto şirketi "Icon" oylamanın şeffaf ve sahtekarlık içermeden yapılabilmesi için bu yönden çalışmalar yapmıştır.

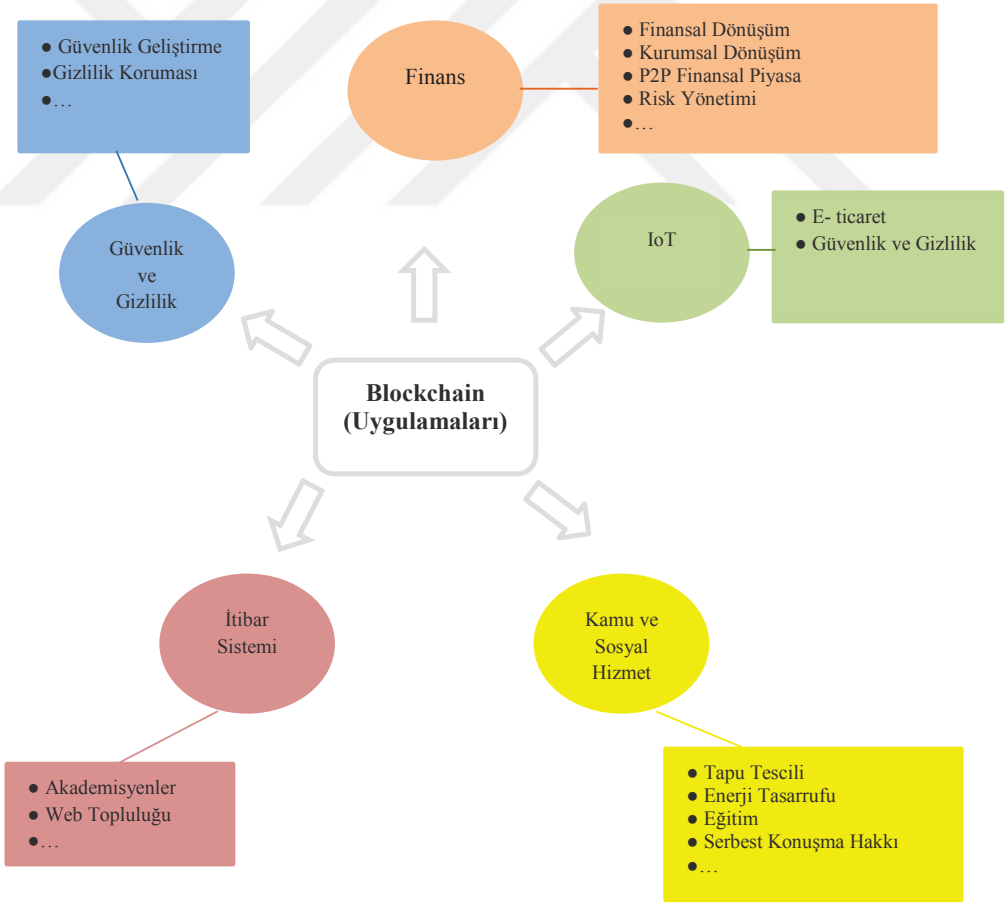
IV. Sağlık sektörü: Blokzincir sağlık sektöründe daha doğru verilerle çalışılabilmesine ve verilere ulaşıp AR-GE çalışmalarının hızlandırılmasına olanak sağlamaktadır.

Aksoy (2018: 32-36) 'da BC kullanım alanlarına çalışmasında şu şekilde yer vermiştir:

V. Tedarik zinciri Yönetimi: BC çok katılımcılı tedarik zinciri yapısının oluşturulmasında son derece verimli çözümler sunabilmektedir. Böylelikle üreticilerin tedarik zincirini BC kullanarak takip etmesi, insan hatalarının ortadan kaldırılmasını sağlamaktadır. Aynı zamanda yüksek maliyetleri fiziki dosyalardan kurtulma, gümrükleme işlemlerinin kolaylaştırılması, kişi veya kurumlara bağlılığın ortadan kalması, ürünün geçirdiği işlem geçmişine ulaşma ve stok yönetimi gibi birçok alanda faydalı olmaktadır.

VI. Abonelik Sistemi: Abonelik sistemi ile satın aldığımız servislerin kullanımında, sayım ve fatura işlemleri için binlerce insanın işgücüne gereksinim duyulmaktadır. BC sisteminde bu tarz işlemlerin kontrolü ve bunun sonucunda verilmesi gereken karşılık tutarı kripto paralar aracılığıyla ödeme sağlanarak kolaylaştırılabilmektedir.

VII. Nesnelerin İnterneti: Blockchain, IoT cihazların herhangi bir merkezi sunucu olmadan birbirleriyle konuşabileceği bir ağ hazırlamaktadır. Böylelikle akıllı aletlerin internet ağında oluşturacağı yük minimum düzeye indirilmekte ve bu cihazların yapacağı veri alışverişi üzerinden yeni gelir modelleri üretmeyi mümkün hale getirmektedir.

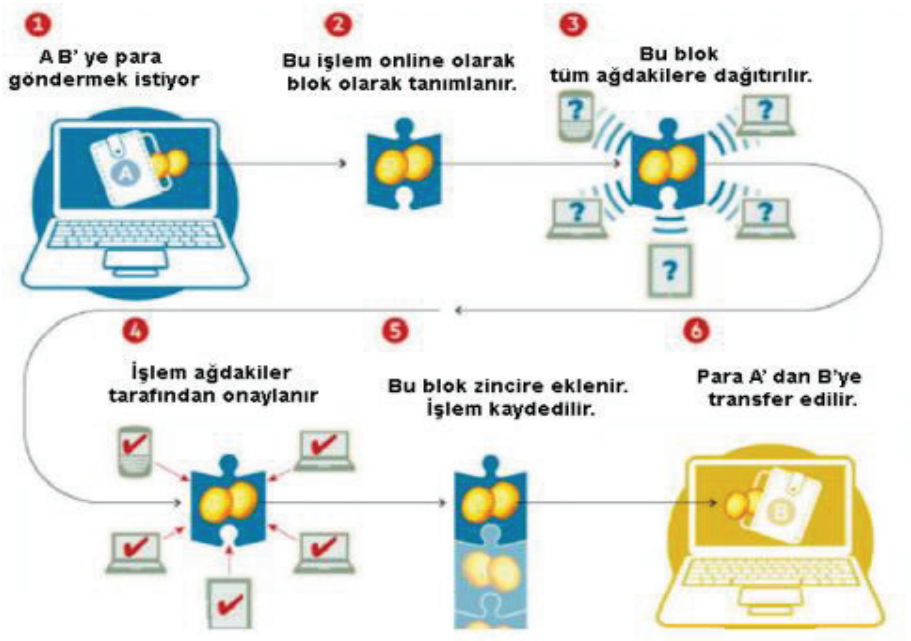


Kaynak: (Zheng, 2018: 363).

Şekil 2: Blockchain Uygulama Alanlarına Genel Bir Bakış

1. 6. 3. Blockchain Teknolojisi Nasıl Çalışır?

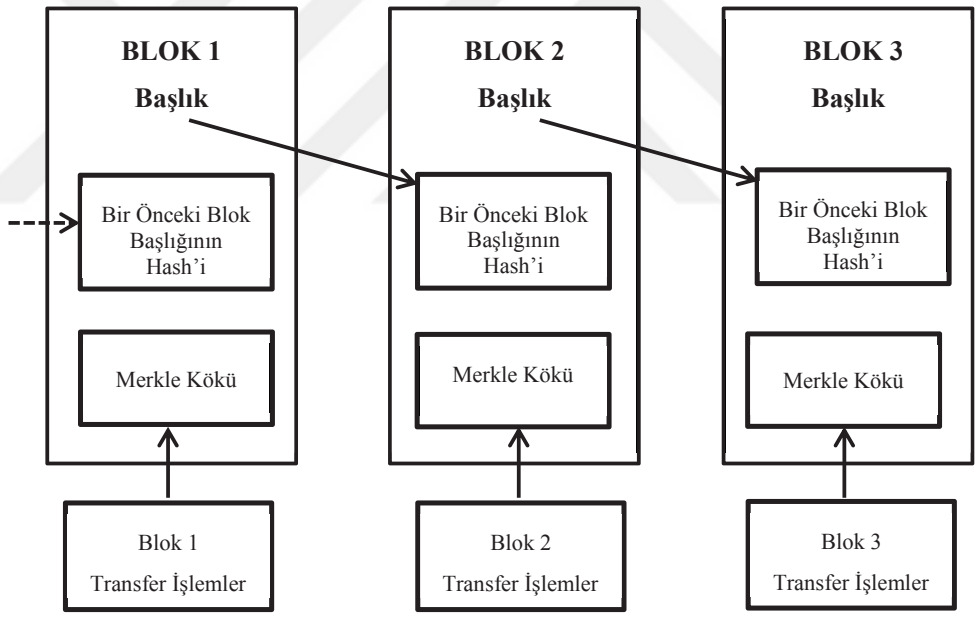
Paranın ortaya çıkmasıyla birlikte yüzyıllardır ticaret sistemi giderek gelişmiş ve bunun sonucu olarak sistemde karmaşıklıklar kendini göstermiştir. Ticaret sisteminindeki bu bilgi karşıklıklarını gidermek, işlemleri doğrulamak ve onaylatmak için de öncelikli olarak hesap defterleri tutulmuş ve teknolojinin gelişmesiyle birlikte bilgisayar üzerinden işlemler yapılmıştır. Ancak bugüne kadar bu işlemlerin gerçekleştirilmesi için banka, devlet ya da muhasebiciler gibi bir aracı kurum ve kuruluşlar ihtiyaç duyulmuştur. Bunların güvenilir oldukları varsayımı altında ise bu aracılara "3. Güvenilir Parti" adı verilmiştir. Blokzincirin mevcut sistemden farklılığı ise bu noktada kendini göstermektedir. Çünkü 3. kişileri ortadan kaldırarak sistemi işletmektedir. Bu noktada Blokchain teknolojisinin işlemesinde üç farklı sistemin birlikte çalıştığı bilinmektedir. Bunlar kriptoloji, bilgisayarlar arası çalışan bir ağ ve son olarak BC protokolüdür. Ancak sistemde işlemin gerçekleştirilebilmesi için en önemli unsurlardan biri, ağa kayıtlı bilgisayarlar vasıtasıyla onay verilmesi gerektiğidir (Konukseven ve Özen, 2018: 72- 73).



Kaynak: (Avunduk ve Aşan, 2018: 373)

Şekil 3: Blokzincirin Genel Çalışma Mantığı

Bu bağlamda blockchain teknolojisi, saklanmak istenen herhangi bir verinin bloklar halinde mühürlenmesi ve bu bloklardan bir zincir oluşturulması mantığına dayanmaktadır. Daha önceden belirlenmiş büyüklükte olan bloklara yazılmakta ve bloklar dolduktan sonra kapatılarak bir önceki bloğun önüne zincirlenerek bağlanmaktadır. Dolayısıyla verilerin geriye dönük bir şekilde değiştirilmesine engel olarak verilerin korunmasını kolaylaştırılmaktadır. Bu noktada sistemlerde gizliliği korumak amacıyla açık anahtar şifreleme teknolojisi sayesinde bir parola gibi gizli tutulan özel bir anahtar ve diğer tüm ajanlarla paylaşılan ortak bir anahtar atanmasıyla sağlanmaktadır. Blockchain'in göze çarpan özelliği ise bu açık anahtarların gerçek dünya kimliğine bağlı olmamasıdır (Pilkington, 2016: 4-5). Bu bilgiler doğrultusunda basitleştirilmiş bir blokchain şeması Şekil 4'te gösterilmiştir.



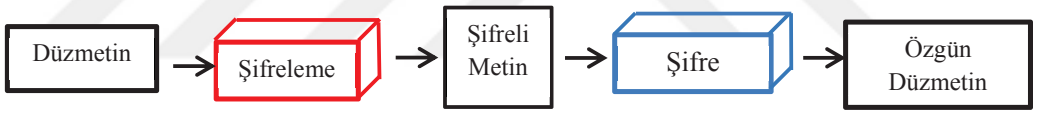
Kaynak: (Aksoy, 2018: 28).

Şekil 4: Basitleştirilmiş Blockchain Şeması

1. 6. 3. 1. Kriptografik Algoritmalar

Kriptoloji, verilerin belirli bir sisteme göre şifrelenip güvenilir bir ortamda alıcıya iletilerek bu şifrenin deşifre edildiği bir şifre bilimi olarak tanımlanmaktadır.

Kripto paralar için önemli bir yere sahip olan kriptolojinin en temel iki unsurunu kriptografi ve kripto analiz oluşturmaktadır. Kriptografide öncelikli olarak verilerin gizliliğinin ve değişmezliğinin korunması yani iletilmek istenen bir mesajın şifrelenme suretiyle üçüncü kişiler tarafından anlaşılmasının engellenmesi hedeflemektedir. Kripto analiz ise, şifrelenmiş bir metnin kırılması yani mesajın sahip olduğu gizli içeriğin tekrar anlaşılabilir duruma getirilmesini hedeflemektedir. Bundan dolayı kriptografiyi İngilizcede "encryption" kripto analizi ise "decryption" kelimeleri karşılamaktadır. Her iki durumda ise şifreleme işleminde matematiksel işlemlerden ve formüllerden yararlanılması gerekmektedir. Bundan dolayı kriptoloji eski zamanlardan bu zamanda kadar bilginin korunmasında en etkili yollardan biri olmuş ve bilginin sahibi dışındaki kişilere ulaşımı engellenmiştir. (Aslantaş Ateş, 2016: 352). Kriptolojik şifrelem yöntemindeki şifreleme ve deşifreleme işlemi Şekil 5'te net bir şekilde gösterilmiştir.



Kaynak: (İşler, Takaoğlu ve Küçükali, 2019: 74).

Şekil 5: Şifreleme ve Deşifre İşlemi

Kriptolojide şifrelenmemiş metin, düz metin olarak adlandırılmaktadır. Düzmetin; verileri, sayısallaştırılmış ses dizisi ve video resmi gibi birçok unsuru bünyesinde bulundurmaktadır. Eğer mesaj iletilirken bilgisayarlardan yararlanılırsa her koşulda, düz metin sayısallaştırılmış ve elektronik ortama aktarılırmış olacaktır. İşlemsel mantık doğrultusunda ilk olarak açık metin şifrelenerek şifrelenmiş metine dönüştürülürken, şifrelenmiş metin ise bu şifrelenin çözülmesiyle yani deşifre edilmesiyle tekrardan açık metine dönüştürülmektedir (Yılmaz, 2007: 138-139).

Kriptografi, bu şekilde gizliliği, doğruluğu, bütünlüğü ve özgünlüğünün etkisiyle birçok alanda kendine yer bulmayı başarmıştır. Bu noktada özellikle kablolu ve kablosuz ağlarda veri aktarımının istenmeyen kişilerce görülmesinin engellenmesi, bilgisayar sistemlerindeki verilere yetkisiz erişimlerin önüne geçilmesi ve güvenli bir

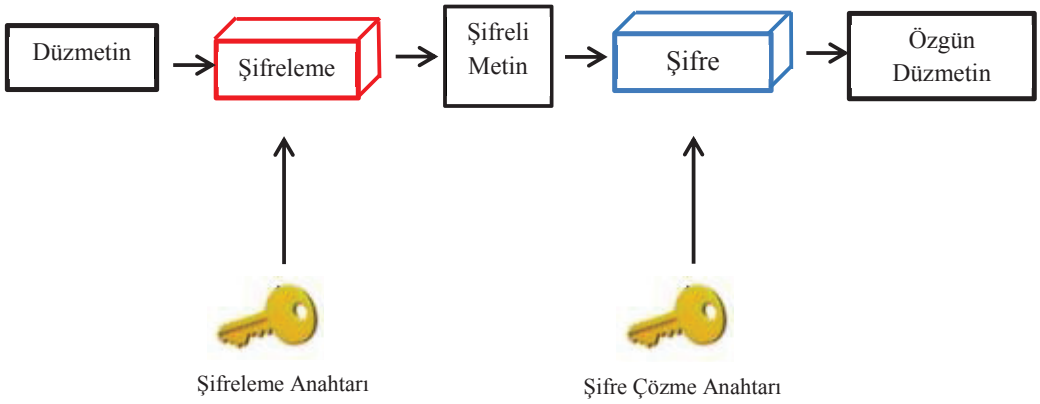
şekilde e-ticaret işlemlerinin gerçekleştirilmesi gibi sağladığı avantajlardan dolayı kripto paralarda da kendine önemli bir yer tutmuş ve güvenliğin sağlanmasında en etkili unsurlardan biri olmuştur (Yerlikaya, Buluş ve Buluş, 2006).

Kripto paralarda ve genel şifreleme sisteminde bilginin deşifre edilebilmesi için anahtar olarak isimlendirilen bir aletten yararlanılmaktadır. Şifreleme biliminde ise bu yönde simetrik ve asimetrik şifreleme algoritmaları olmak üzere iki farklı sistemden yararlanılmaktadır. Bu noktada bilginin şifrelenmesinde ve deşifre edilmesinde, simetrik şifreleme yöntemiyle aynı anahtar kullanılabilirken; asimetrik şifreleme yönteminde olduğu gibi farklı anahtarlarda kullanılabilmektedir. Ancak bu durumlar dışında her iki yöntemden de birlikte yararlanılabilecek melez şifreleme yöntemi de bulunmaktadır (Yılmaz, 2007: 139).

1. 6. 3. 1. 1. Asimetrik Şifreleme

Asimetrik anahtar şifreleme tekniği, şifreleme ve şifreyi çözme sürecinde farklı anahtarların kullanıldığı bir teknik olarak nitelendirilmektedir. Bu iki anahtar ise birbirleriyle matematiksel bir ilişki doğrultusunda bağlılık göstermekle birlikte birbirlerinden farklıdırlar. Dolayısıyla birbirlerinin yerine kullanılamayıp sadece birbirlerini tamamlayıcı özellik sergilemektedirler. Bu anahtarlardan biri halka açık iken bir diğeri gizli tutulmakta ve açık anahtar (public key) şifrelemek için kullanılırken, özel anahtarlar (private key) şifreyi çözmek için kullanılmaktadır. Ancak burada önemli olan nokta eğer şifreleme yani kilitleme anahtarı ilk yayınlandıysa sistem, halktan kilit açma anahtarının kullanıcısına iletişim olanağı sağlamaktadır. Tam tersi eğer şifre çözme yani kilit açma anahtarı önce yayınlandıysa o zaman sistem, özel anahtar sahibi tarafından kilitlenen belgelerin imza doğrulayıcısı olarak hizmet gerçekleştirmektedir (Tripathi ve Agrawal, 2014: 73).

Asimetrik şifreleme yöntemi çalışmanın bundan sonraki kısmında daha ayrıntılı bir şekilde anlatılmıştır. Ancak öncelikli olarak asimetrik şifreleme yöntemindeki şifreleme ve deşifreleme yöntemlerinin daha net analışılması ve bir anahtar ile şifreleme yapılırken bir başka anahtarla şifre çözülme süresinin görülebilmesi için, genel şifreleme mantığı doğrultusunda, bu süreç Şekil 6'da gösterilmiştir.



Kaynak: (Katrancı ve Özdemir, 2013: 162).

Şekil 6: Asimetrik Şifreleme Şeması

Asimetrik şifreleme tekniğini önemli yapan unsurlardan biri simetrik şifreleme algoritmalarının en önemli sorunlarından olan anahtar dağıtım problemini ortadan kaldırmasıdır. Ancak çözülmesi zor hatta özümü olmayan matematiksel problemlerin üzerine kurulduklarından dolayı çok sayıda işlem yapılmasına neden olmaktadır. Bu şekilde işlem sayılarında artışlar meydan geldikçe çalışma performansı üzerine yansımakta ve bu performans oldukça düşük olmaktadır. Bu teknik sadece şifreleme amaçlı değil aynı zamanda doğrulama amaçlı olarak da dijital (elektronik) imzalarda da kullanılabilmektedirler. (Gençoğlu, 2017: 20).

Kripto paralarda tercih edilen şifreleme tekniği asimetrik algoritmalı şifreleme tekniğidir. Asitmetrik şifrelemenin en yaygın algoritmaları ise RSA (Rivest-Shamir- Adleman), Eliptik Eğri Algoritması (ECC), ElGamal, ve Diffie- Hellman (DH), DSA (Digital Signature Algorithm) olarak verilmektedir (Yılmaz ve Ballı, 2016: 20).

1. 6. 3. 1. 1. 1. RSA Asimetrik Şifreleme Algoritması

RSA, 1978 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından tasarlanmıştır. Anahtar değişimi, dijital imzalar ve veri bloklarının şifrelenmesi için bilinen en iyi açık anahtar şifreleme sistemlerinden biridir. RSA algoritması değişken boyutlarda şifreleme bloğu ve değişken boyutlarda anahtarlar kullanmaktadır. Bir blok şifreleme sistemi olan ve sayı teorisine dayanan asimetrik bir şifreleme

sistemidir. Açık ve özel anahtarları üretmek için iki asal sayı kullanmaktadır. Ayrıca bu iki farklı anahtar şifreleme ve şifre çözme amacıyla kullanılmaktadır. Burada gönderici, alıcı ile olan ortak anahtarlarını kullanarak mesajı şifrelemekte ve bu şifrelenen mesaj alıcıya iletildiğinde, alıcı kendi özel anahtarlarını kullanarak şifreyi çözebilmektedir. Aynı zamanda RSA işlemleri anahtar üretimi, şifreleme ve şifre çözme olmak üzere üç geniş adıma ayrıştırılmaktadır (Singh ve Supriya, 2013: 35).

Anahtar Üretimi*:* Veriler şifrelenmeden önce anahtar üretilmeli ve bu birkaç adımlar doğrultusunda gerçekleştirilmektedir. Bu adımlar aşağıda gösterilmektedir:

- Birbirinden bağımsız olan iki adet p ve q asal sayıları yaklaşık aynı büyüklükte olacak şekilde üretilmektedir.
- n=p.q ve Q= (p-1). (q-1) değeri hesaplanmaktadır.
- Rastgele bir tamsayı olmak üzere e, OBEB (e, Q) =1 ve 1 < e < Q şartları sağlamak üzere üretilmektedir.
- Kapsamlı bir Öklid Algoritması kullanılarak yegâne bir tamsayı olmak üzere d, 1 < d < Q ve e.d ≡1 mod(Q) şartları sağlamak üzere üretilmektedir.
- Bilgiyi alacak kişinin açık anahtarı (n, e) ve gizli anahtarı (d) olmaktadır.

(Akben ve Subaşı, 2005: 36).

Şifreleme: Bir "B" alıcısına mesaj göndermek isteyen bir "A" göndereni olduğu varsayımı altında, mesajı gönderecek kişinin izleyeceği adımlar aşağıda sıralanmıştır.

- Bilgiyi alacak olan "B" bilgiyi gönderen "A" nın açık anahtarı olan (n, e)'yi alacaktır.
- Düz metin mesaj, pozitif bir tamsayı (M) olarak gösterilmektedir.
- C= m*(mod n) olmak üzere şifreli metin'in değeri hesaplanmaktadır.
- Bilgiyi gönderecek olan "A" şifrelenen metin olan "C" yi bilgiyi alacak kişiye yani "B" ye göndermektedir.

(Goshwe, 2013: 11).

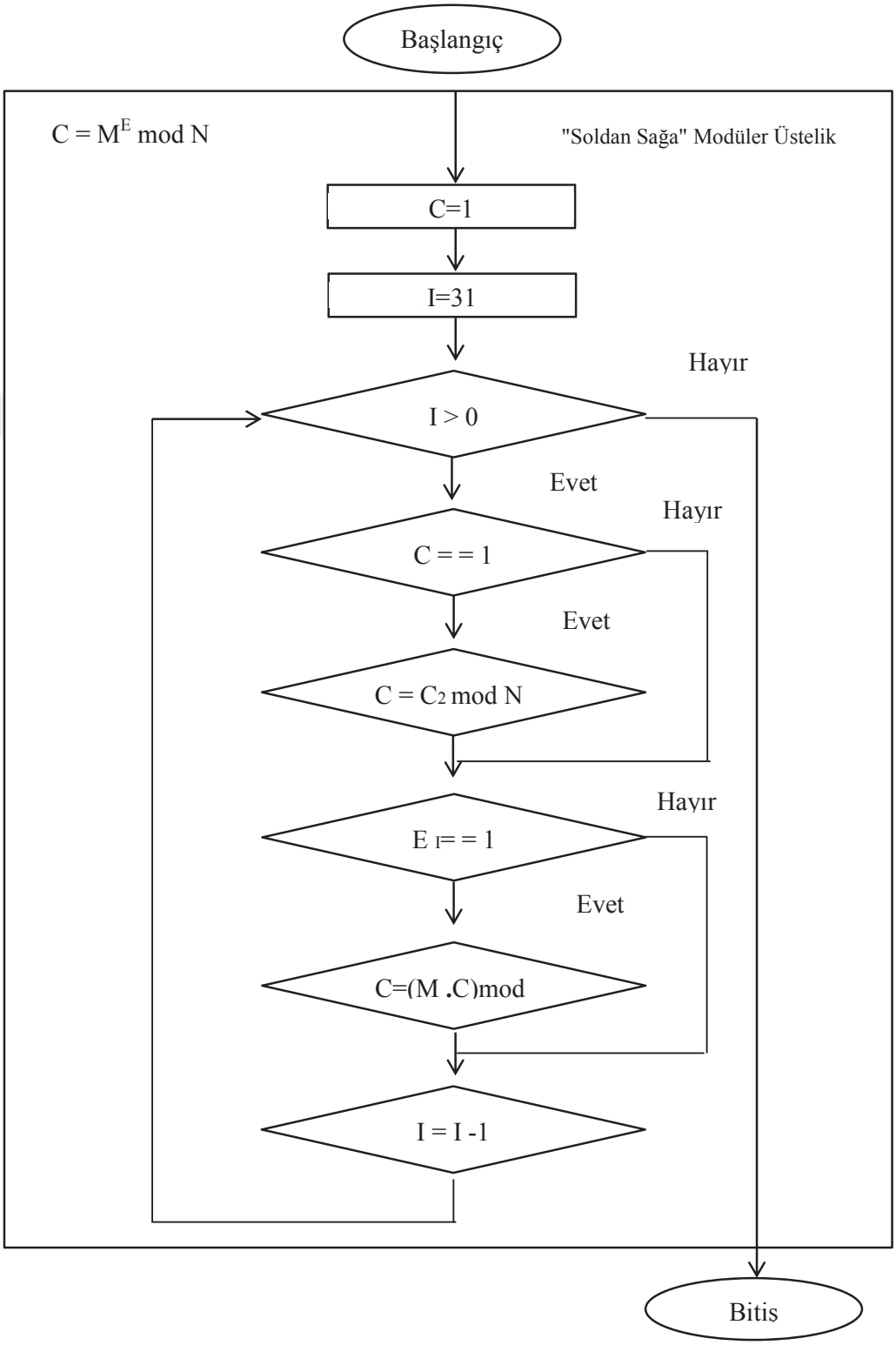
Şifre Çözme: Alıcı şifresini çözmek için aşağıdaki yöntemi kullanmaktadır:

- Düz (orijinal) metin $M= C^d$ (mod n) olacak şekilde hesaplanarak bilgiyi alacak kişi tarafından elde edilmektedir.

(Minni vd., 2013: 1).

Bu algoritmalarda özellikle iki asal sayının çarpımını kullanarak bir anahtar oluşturulmasının asıl sebebi, iki asal sayının çarpımını asal çarpanlara ayırmanın asal olmayan sayılara göre asal çarpanlara ayrılmasından çok daha kolay olmasıdır. Buradaki formüller işleme koyulduğu zaman en uzun süreyi alan işlem, üst alma ve mod bulma işlemleridir. Dolayısıyla süreci hızlandırabilmek amacıyla rastgele seçilen bir tamsayı değerinin küçük veya hesaplanması kolay bir değer seçilmesi gerekmektedir. Ancak değerin küçüklüğü ve tekrarlı kullanılması güvenliği azaltmaktadır. Bu durumu engelleyebilmek amacıyla kullanılabilcek metod ise uzatılmış Öklid algoritması ve modüler üs alma metodlarıdır. Bu metodlar kullanılarak büyük sayılarla kısa sürede şifreleme yapılabilmektedir. Sonuç olarak açık anahtarlı şifreleme algoritmalarında güvenliğin sağlanmasında anahtar uzunluğu oldukça önemlidir. Bu doğrultuda RSA şifreleme algoritmasının güvenliği için 512 bit ve daha uzun anahtarların kullanılması önerilmektedir. Böylelikle kullanılan şifreleme yöntemi güvenliğin sağlanmasında daha etkili olmaktadır (Yerlikaya vd., 2013: 97-103).

RSA algoritmasında bu özelliklerin yanı sıra birçok kusurun mevcut olduğunun da belirtilmesi gerekmektedir. Örneğin anahtar tasarımı için küçük p ve q değerleri seçildiği zaman şifreleme işlemi çok zayıf hale gelmektedir. Bundan dolayı da biri rastgele olasılık teorisini, saldırıları kullanarak verilerin şifrelerini çözebilmektedirler. Diğer yandan eğer büyük p ve q uzunlukları seçilirse daha fazla zaman harcanmış olmakta ve bu durum performansın düşmesine neden olmaktadır. Ayrıca algoritmanın p ve q için eşit uzunluklara ihtiyaç duyması, uygulamada gerçekleştirilmesi zor bir şart olarak kendisini göstermektedir. Bu tür durumlarda farklı tekniklerin uygulanmasını beraberinde getirmektedir. Dolayısıyla fazla işlem süresi alarak sistemin genel giderlerinin artmasına neden olmaktadır. Bu dezavantajlardan dolayı ticarette kullanım için çok fazla tercih edilen teknikler arasında yer almamaktadır (Singh ve Supriya, 2013: 35). RSA şifreleme algoritmasının şifreleme ve şifre çözme ortak akış şeması Şekil 7'de gösterilmiştir.



Kaynak: (Mahajan ve Sachdeva, 2013: 19).

Şekil 7: RSA Şifreleme ve Şifre Çözme Akış Şeması

1. 6. 3. 1. 1. 2. Dijital İmza Algoritma (DSA) Yöntemi

Dijital İmza Algortiması National Institute of Standartds and Technology (NIST) tarafında "Federal İnformation Processing Standard (FIPS)" yani "Federal Bilgi İşlem Standardı" altında bir güvenlik standardı yayınlanmasıyla 1991 yılının Ağustos ayında tanıtılmıştır. DSA, ElGamal şifreleme algoritmasının bir varyansı olup ayrık yani kesikli logaritma problemini baz almaktadır. İmzalama işleminde ise SHA-1 kullanılmaktadır (Harn, Mehta ve Hsin, 2004: 198).

DSA yönteminde güvenlik asimetrik algoritmaları kullanarak oluşturulan anahtarlar sayesinde gerçekleştirilmektedir. Asimetrik algoritmalar kullanıcıya açık anahtar ve gizli anahtar olmak üzere iki anahtar tanımlamakta olup DSA bu anahtarlarla ilgili ilk olarak 512 bit anahtar uzunluğuna sahip olacak şekilde tasarlanmış ancak daha sonra 2^{1023} ile 2^{1024} arasında bir değer almasına yani 1024 bit uzunluğunda olmasına karar verilmiştir. Diğer yandan burada açık anahtar, gizli olmayan ve herkesin erişim sağlayabileceği anahtar türüyken özel anahtar sadece dijital imzanın sahibi olan kişi tarafından bilinen bir anahtar olup bu anahtar bireylerin dijital imzasıdır. Alıcı kendisine gönderilen dijital imzalı verilerin doğru kişi tarafından gönderilip gönderilmediğini ve veride bütünlüğün sağlanıp sağlanmadığını anlamak için gönderen kişinin gizli anahtarının bir karşılığı olan açık anahtarı kullanması gerekmektedir (Akçeşme ve Sönmez, 2008: 131).

Dijital imza yöntemi güvenlik açısından genellikle iki tamamlayıcı algoritmayı tanımlamaktadır. Bunlardan biri imzalama bir diğeri de doğrulama algoritmasıdır. İmzalanana işlemin çıktısı ise dijital imza olarak ifade edilmektedir. Bu noktada DSA algoritmasının net bir şekilde anlaşılabilmesi için dijital imzanın da iyi bir şekilde bilinmesi gerekmektedir. Bu bağlamda dijital imza kimlik doğrulama amacıyla mantıksal bir bağlantı çerçevesinde kullanılan elektronik bir veri ya da veri ekleme yöntemidir. DSA dijital imzası bir çift büyük sayıdır ve bilgisayarda ikili basamakların dizeleri olarak gösterilmektedir. Dijital imzalama da öncelikli olarak, herhangi bir elektronik dokümana eklenen imzalama verisinin bir kişiye ait olup olmadığının kanıtlanması amaçlanmaktadır. Dijital imza, imzalayan kişinin kimlik doğruluğunun kanıtlarken aynı zamanda imzalanan bir verinin içeriğine müdahale edilip edilmediğini yani bu verilerin bütünlüğünün bozulup bozulmadığını ortaya koymaktadır. İmzalayanın kimliğini ve verilerin bütünlüğünü doğrulamak için de bir

dizi parametreler kullanarak hesaplama yapmaktadır (Alajbegović ve Jamak ve Zečić, 2006: 665).

Bu noktada (Sarısakal, Marangoz ve Uçan, 2001: 173); p, q ve g tamsayılarının herkes tarafından kullanılabileceğini ve x gizli anahtar, y açık anahtar olmak üzere k parametrelerinin her imza için yeniden üretilmesi gerektiğini belirtmiştir. DSA parametrelerini aşağıdaki gibi ayrıntılı bir şekilde açıklamıştır:

- "P" asal sayı modüldür. $2^{l-1} < P < 2^{L}$, $512 \leq L \leq 1024$ ve L, 64'ün bir katı olmak zorundadır.
- q, (p-1); y sayısının asal çapanıdır. $2^{159} < q < 2^{160}$
- $g = h^{(p-1)/q} \bmod p$ h, $1 < h < (p-1)$ ve $h^{(p-1)/q} \bmod p > 1$ şeklindeki rstgele bir tamsayıdır.
- x herhangi bir sayıdır ve $0 < x < q$ dur.
- $y = g^{x} \bmod p$ dir.
- k herhangi bir sayıdır ve $0 < k < q$ dur.

Bu parametre doğrultusunda anahtar üretimi ve DSA yönteminin iki tamamlayıcı algoritması olan imzalama ve doğrulama işlemleri aşağıda ayrıntılı bir şekilde açıklanmıştır.

Anahtar Üretimi: Dijital imzalama algoritmasında anahtar üretimi için takip edilmesi gereken aşamalar aşağıda verilmiştir:

- $2^{1023} < p < 2^{1024}$ şartını sağlayacak şekilde p asal sayısının seçilmesi gerekmektedir.
- (p-1)'in asal böleni ve $2^{159} < q < 2^{160}$ olacak şekilde q asal sayısı seçilmelidir.
- $1 < h < (p-1)$ ve $h^{(p-1)/q} \bmod p > 1$ şartını sağlamak üzere h seçilmektedir.
- $g = h^{(p-1)} \bmod p$ değerinin hesaplanması gerekmektedir.
- $0 < x < q$ şartını sağlayacak şekilde rastgele x tamsayısı belirlenmektedir.
- $y = g^{x} \bmod p$ değerinin hesaplanması gerekmektedir.
- Tüm bu işlemlerden sonra açık anahtar (p, q, g, y), ve özel anahtar (x) olmaktadır.

(Saygı ve Yeşil, 2006: 4).

İmzalama: DSA şifreleme yönteminde imzalama işleminin gerçekleştirilebilmesi için gerekli aşamalar şunlardır:

- $m \in M$ olacak şekilde bir mesaj (m) seçilmesi gerekmektedir.
- m' = SHA- 1 (m) değeri bulunmaktadır.
- $0 < k < q$ olacak şekilde bir k tamsayısının seçilmesi gerekmektedir.
- $r = (g^k \bmod p) \bmod q$ değeri hesaplanmaktadır.
- $s = (k^{-1} (m' + x \cdot r)) \bmod q$ bulunmaktadır.
- (r, s), m mesajın son hazırlanmış halidir.

(Sarıkaya, 2005: 46).

İmza Doğrulama: İmzalama aşamasından sonra imza doğrulama işleminin gerçekleştirilmesi için gerekli aşamalar aşağıda gösterilmiştir:

- İmzalama yapan kişini açık anahtarı öğrenilmektedir. (p, q, g, y)
- $o < r < q$ ve $0 < s < q$ değeri doğrulanmaktadır.
- m' = SHA-A (m) değeri bulunmaktadır.
- $w = s^{-1} \bmod q$ bulunmaktadır.
- $u = (w \cdot m') \bmod g$ ve $v = (r \cdot w) \bmod q$ değeri bulunmaktadır.
- $v = ((g^u y^v) \bmod p) \bmod q$ bulunmaktadır.
- v = r ise imza doğrulanmaktadır.

(Saygı ve Yeşil, 2006: 4).

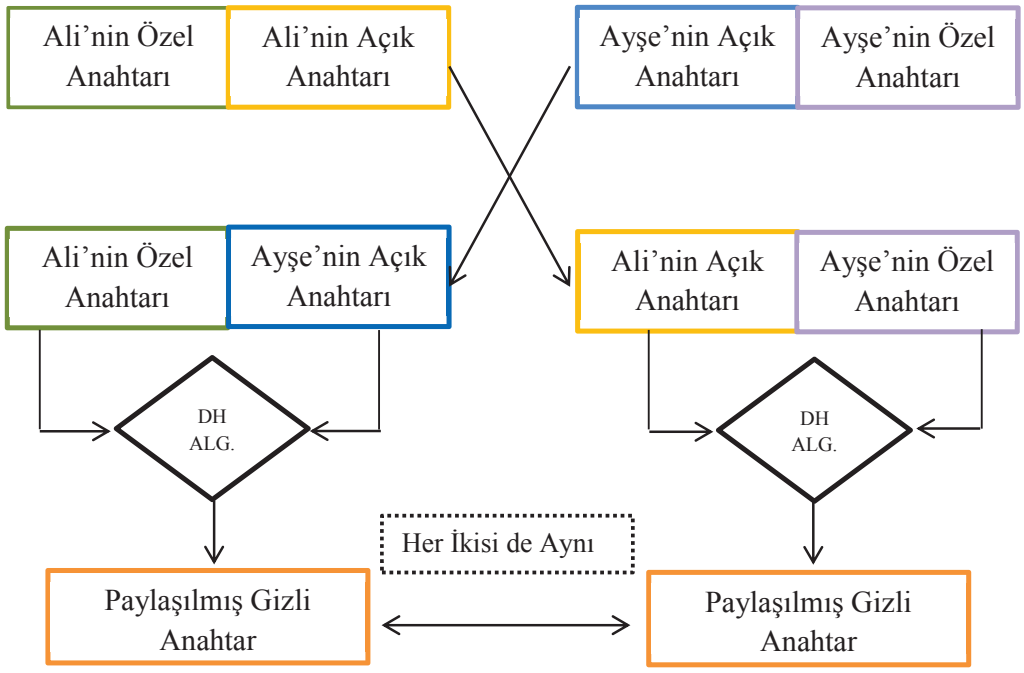
1. 6. 3. 1. 1. 3. Diffie- Hellman Asimetrik Şifreleme Yöntemi

Diffie-Hellman anahtar değişimi için kulllanılan özel bir yöntemdir ve bu yöntem şifreleme alanında uygulanan en önemli değişimlerden biridir. Diffie-Hellman anahtar değişiminde, iki taraf arasında güvenli olmayan bir kanal üzerinden ve birbirleri ile ilgili önceden bilgi sahibi olmayan kişiler arasında kararlaştırılmış bir gizli anahtar paylaşarak güvenli iletişim için uygun bir ortam hazırlamayı amaçlamaktadır. Yani algoritma iki varlık arasında gizli bir anahtar sağlayarak

kişilerin birbirleri ile paylaşacakları bilgileri simetrik bir şifrelemeyle şifreleyerek güvenli bir bilgi alışverişine olanak sağlamayı amaçlamaktadır (Zanjani, 2014: 8).

Diffie-Hellman algoritmasında en önemli nokta algoritmaların kendisinin verileri şifrelememesidir. Bunun yerine gönderen ve alıcı için ortak olan gizli bir anahtar oluşturulmaktadır. Burada matematiksel olarak birbirine bağlı olan işlemler aracılığıyla iki taraf bağımsız olarak aynı özel anahtarı üreterek, asimetrik şifreleme algoritmasında kullanılmak üzere, bir oturum anahtarı oluşturabilmektedir. Yani iki tarafın kullanımı için bir anahtar üzerinde anlaşılmaktadır. Bu durum literatürde "key agreement" yani " anahtar sözleşme" olarak açıklanmaktadır (Ahmed vd., 2012: 69).

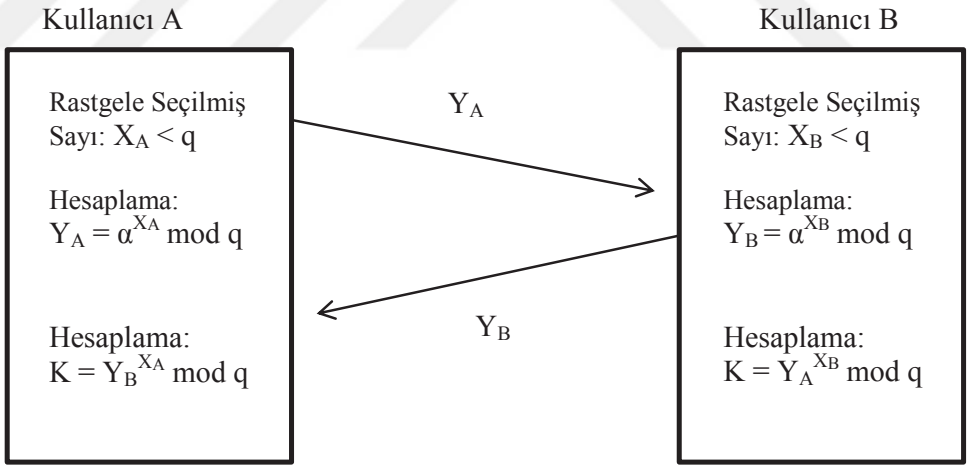
Bir anahtar şifreleme algoritması olarak Diffie-Hellman modeli Whitfield Diffie ve Martin Hellman tarafından 1976 yılında gerçekleştirilen bir öneriyle birlikte ortaya çıkmıştır. Diffie-Hellman algoritmasında eğer gönderen alıcıyla iletişim kurmak istiyorsa, iletilmek istenen mesajı hem özel anahtarıyla hem de gönderenlerin açık anahtarı ile şifrelenmektedir. Sonraki aşamada ise alıcı taraf, alıcı ortak anahtarlarının şifresini çözmektedir (Tirhani ve Ganesan, 2014).



Kaynak: (Durairajan ve Saravanan, 2014: 4360).

Şekil 8: Diffie-Hellman Mekanizması

Diffie- Hellman şifreleme algoritmasının, güvenlik sağlamadaki etkinliği ve gücü ayrık logaritmaların hesaplanmasının oldukça zor bir işlem olmasından kaynaklanmaktadır. Algoritmanın mekanizmasında "q" bir asal sayı ve bunun ilke kökü olan "α" açık sayıları bulunmaktadır. Bu noktada birbirleriyle bilgi alışverişinde bulunmak isteyen A ve B kişilerinin olduğu varsayımı altında, A kişisi ($X_A < q$)olmak üzere rastgele bir sayı seçmekte ve daha sonra ($Y_A = \alpha^{X_A} \bmod q$) değerini hesaplanmaktadır. Benzer şekilde B kişisi de öncelikli olarak ($X_B < q$) şeklinde rastgele bir sayı seçmekte ve A kişisinde olduğu gibi sonraki aşamada ($Y_B = \alpha^{X_B} \bmod q$) değerini hesaplamaktadır. X değerinin Bu durumda hem A hem B kişisi X değerinin kendine özel olacak şekilde gizli tutarken Y değerini iki tarfta birbirlerine göndermektedirler. En son aşamada ise karşı taraftan paylaşılan özel anahtara A kişi ($K = Y_B^{X_A} \bmod q$) ve B kişisi ($K = Y_A^{X_B} \bmod q$) değerlerini hesaplayarak ulaşmaktadır (Karzan, 2013: 20). Açıklanan bu bilgiler Şekil 9'da özet olarak gösterilmiştir.



Kaynak: (Durairajan ve Saravanan, 2014: 4361).

Şekil 9: Diffie-Hellman Algoritması

1. 6. 3. 1. 1. 4. Eliptik Eğri Kriptoloji Algoritması

Eliptik eğri şifreleme ilk olarak 1985 yılında Neal Koblitz ve Victor Miller öncülüğünde ileri sürülmüştür. Bu şifreleme algoritmasının temeli eliptik eğri ayrık

logaritma problemindeki zorunluklara dayanmaktadır. Ancak bu problemlerin çözümü için geliştirilmiş yarı üssel algoritmalar henüz mevcut değildir. Asimetrik şifrelemenin en yaygın kullandığı kriptoloji algoritması olan RSA algoritmasından farklı olarak eliptik eğri şifreleme sisteminde güvenlik için daha kısa bir anahtar uzunluğu kullanılmaktadır. Örneğin RSA algoritmasında 128 byte'lık bir anahtar kullanılarak sağlanan bir güvenlik, eliptik şifreleme algoritmasında 20 byte ile sağlanabilmektedir. Diğer yandan şifrelemenin bu alanının kullanılabilmesi, elemanlar ve birleştirme kurallarını tanımlamaya olanak sağlayan tekniklerin mevcut olduğu gruplar sayesinde gerçekleşmektedir (Yavuz, 2008: 7).

(Hassanpur, 2015) bu noktada K' yı bir cisim olarak değerlendirerek a, b, c, d, e, x, y'nin K cisminin elemanı olduğu varsayımı altında eliptik eğrinin genel denklemini aşağıdaki denklemler doğrultusunda belirtmiştir:

$$Y^2 + axy + by = x^3 + cx^2 + dx + e \qquad (2)$$

bu doğrultuda ECC'nin genel denkleminin afin dönüşümleri kullanılması sonucunda gerçekleşen char (K) = 2 durumu varsayımı sonucunda ise;

$$Y^2 + ay = x^3 + bx + c \quad \text{ya da} \quad y^2 + xy = x^3 + ax^2 + b \qquad (3)$$

şeklinde bir denkleme dönüşmektedir. Diğer yandan, char (K) = 3 varsayımı altında ise mevcut denklem;

$$Y^2 = x^3 + ax^2 + bx + c \qquad (4)$$

denklemi haline gelmektedir. Aynı zamanda, char (K) $\neq$ 2,3 şeklinde bir eliptik eğri varsayımı gerçekleşebilmektedir. Bunun sonucunda gerçekleşecek denklemli eliptik eğri E ile gösterilirse; F (x) = x^3 + ax + b olduğu varsayımı altında r_1, r_2, r_3, f (x) = 0 denkleminin kökleri olması durumunda f polinomunun diskiriminantı aşağıda gösterilmiştir;

$$\Delta (f) = \left(r1 - r2 \right)^2 \left(r2 - r3 \right)^2 \left(r1 - r3 \right)^2 \quad (5)$$

f polinomunun diskiriminantı, $\Delta(f) = 4a^3 + 27b^2$ şeklinde ifade edilebilmektedir. Aynı zamanda mevcut f (x) polinomunun katlı kök içerip içermediğinin anlaşılması da önemli bir konudur ve bu noktada polinomun disciriminantına bakılarak katlı kök olup olmadığına karar verilmektedir. Bu durumda eğer Δ (f) $\neq$ 0 olduğu anlaşılırsa polinomun katlı kök olmadığı sonucuna ulaşılmaktadır.

Eliptik eğri şifreleme algoritmasının temellerini oluşturan matematiksel yapı da bu noktada önem arz etmektedir. Altyapıda bahsedilebilecek en önemli konu ise sonlu alanlardır ve toplama-çarpma olmak üzere iki işlemden oluşmaktadır. Diğer yandan işlemlerin gerçekleştirilmesinde belirli özelliklerin gerçekleştirilmesi gerekmektedir. Bu özellikler eliptik eğri için sonlu bir alanın q elemanına sahip olması ve bu q elemanının da asal sayının üssü olması gerekmektedir. Bu özellik sayesinde her q elemanına ait tek bir sonlu alan bulunmasına neden olmakta ve q elemanına sahip olan alan ise F_q matematiksel ifade ile gösterilmektedir. Bu özellik bağlamında eliptik eğrilerde asal sonlu "F_p" ve karakteristik iki "F_2" olmak üzere iki tür sonlu alan F_q kullanılmaktadır (Bozkurt, 2005: 12).

Eliptik eğrinin bu genel özellikleri kripto para sürecinde de önemli bir unsur olan anahtar üretme, şifreleme ve şifre çözme tekniği gibi aşamaların nasıl oluştuğu sorularını akla getirmektedir. Bu nokda ECC algoritmasındaki anahtar üretimi, şifreleme ve şifre çözme yöntemlerini (Akben ve Subaşı, 2005: 37)' de aşamalar halinde aşağıdaki gibi açıklanmıştır.

Anahtar Üretimi: Eliptik Eğri Şifreleme yönteminde anahtar üretimi için gerekli olan aşamalar aşağıda ayrıntılı bir şekilde sıralanmıştır:

- Rastgele bir tamsayı olarak [1, n-1] olacak şekilde seçilmektedir.
- Q = d. P denklemi üzerinden hesaplama yapılmaktadır.
- Bu noktada bilgiyi alacak kişinin açık anahtarı Q olurken özel anahtarı d olarak gösterilmektedir.

Şifreleme: Anahtar üretimi işlemi gerçekleştikten sonra şifreleme ile bilginin korunması için takip edilmesi gereken yollar aşağıda belirtilmiştir:

- İlk aşamada bilgiyi gönderecek kişi bilgiyi alacak kişinin açık anahtarını yani Q' yu elde etmektedir.
- Mesaj (m)' nin, F_q'nun elemanı olmasına dikkat edilecek şekilde, bir tamsayı haline dönüştürülmesi gerekmektedir.
- Bu noktada rastgele bir tamsayı olarak k, [1, n-1] olacak şekilde seçilmektedir.
- $(x_1, y_1) = k.P$ hasaplanması yapılmaktadır.
- İşlem aşaması bağlamında $(x_2, y_2) = k. Q$ hesaplanmaktadır. Ancak bu noktada dikkat edilmesi gereken unsur eğer $x_2 = 0$ değerini alırsa önceki adımlar biri olan üçüncü adıma geri dönülmesi gerekmektedir.
- Şifrelenmiş metin $c= m. x_2$ formülü ile hesaplanmaktadır.
- Şifrelenen metin bilgiyi alacak kişiye gönderilmektedir.

Şifre Çözme: Şifrelenmiş bilgiyi alan kişinin şifre çözmesi için izlenmesi gereken yollar vardır. Bunlar aşağıda açıklanmıştır:

- Bilgi alacak olan kişi, özel anahtarını kullanılıp $(x_2, y_2) = d. (x_1, y_1)$' i hesaplayarak şifreyi çözme aşamasının ikinci aşamasına geçmektedir.
- Son olarak $m = (c. x_2)^{-1} \bmod n$ denklemi ile şifrelenmiş metinin çözümüne ulaşmaktadır.

1. 6. 3. 1. 1. 5. ElGamal Şifreleme Algoritması

ElGamal kriptoloji yöntemi 1985 yılında ayrık logaritmik problemler üzerine kurulmuş açık anahtar şifreleme yöntemi olarak bilinmektedir. Güvenliği de bu ayrık logaritma problemine dayanmaktadır. Şifreleme ve sayısal imza algoritmalarından oluşmaktadır. Şifre sistemi Diffie-Hellman anahtar anlaşması (Diffie-Hellman Key Aggrement)'na dayanmaktadır. ElGamal yönteminde herkes kendi açık anatarını ve dolayısıyla özel anahtarını oluşturmaktadır (Dülgerler ve Sarısakal, 2003: 802). Buna bağlı olarak anahtar üretimi, şifreleme ve şifre çözme aşamaları aşağıda gösterilmiştir:

Anahtar Üretimi: ElGamal yönteminde anahtar üretimin gerçekleştirilebilmesi için izlenmesi gereken yollar aşağıda gösterilmiştir:

- Oldukça büyük bir asal sayı olan "p" sayısı seçilir.
- a < p olacak şekilde bir "a" sayısı seçilmekte ve rastgele bir "b" sayısı belirlenmektedir.
- a^b mod p sayısı seçilip "Y" olarak gösterilmektedir. Yani $Y = a^b \bmod p$ dir.
- Açık anahtar (a, p, Y); özel anahtar (b) olmaktadır.

(Sarıkaya, 2005: 42).

Şifreleme: Şifreleme için gerekli aşamalar aşağıda gösterilmiştir:

- "m" mesajı $0 \leq m \leq p-1$ şartını sağlayacak şekilde bir tamsayı olarak kabul edilmektedir.
- $1 \leq k \leq p-2$ değerini sağlayan rastgele bir "k" tamsayısı seçilmektedir.
- $T = a^k \pmod p$ ve $S = m \cdot (a^b)^k \pmod p$ değerleri hesaplanmaktadır.
- Bunun sonucunda (T, S) "m" mesajı için şifrelenmiş halini göstermektedir.

(Hassanpour, 2015: 58).

Şifre Çözme: Şifrelenen bir metnin çözülmesi ve doğrulanması için izlenmesi gereken aşamalar aşağıda aşamalar halinde açıklanmıştır:

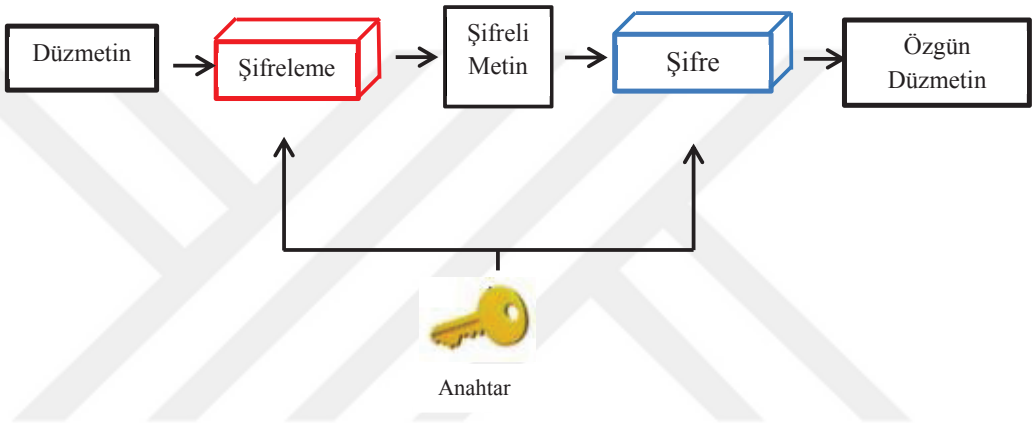
- Gönderenin açık anahtarı (a, p, Y) elde edilmektedir.
- $1 \leq T \leq P-1$ olduğu doğrulanmaktadır.
- $a^m \bmod p = Y^T T^S \bmod p$ ile şifre doğrulanmaktadır.

(Sarıkaya, 2005: 43).

1. 6. 3. 1. 2. Simetrik Şifreleme

Simetrik anahtar şifreleme algoritması, düz metnin şifrelenmesi ve şifrelenen metnin çözülmesi için aynı şifreleme anahtarının kullanıldığı bir algoritmadır. Bilginin ya da verinin şifrelenmesi için gönderen kişi tek bir anahtarı ve şifreleme algoritmasını kullanmakta ve aynı şekilde bu veriyi alan kişide aynı anahtarı ve şifre algoritmasını kullanarak şifreyi çözmektedir. Ancak bu noktada gizliliğin

sağlanabilmesi için anahtarın ve algoritmanın taraflarca gizli tutulması gerekmektedir. Aksi takdirde bir başka kişi bu gizli anahtarı ve algoritmayı öğrendiğinde bilginin güvenliği sağlanamamaktadır. Dolayısıyla simetrik şifrelemede anahtarlar, özel bir bilgi bağlantısını devam ettirip sürdürebilmek için her iki taraf arasında paylaşılan bir sırrı temsil etmektedir (Sasi, Dixon ve Wilson, 2014: 2). Simetrik şifreleme şeması Şekil 10'da gösterilmiştir.



Kaynak: (Katrancı ve Özdemir, 2013: 162).

Şekil 10: Simetrik Şifreleme Şeması

Simetrik şifrelemenin bu işleyişinin diğer şifreleme türleriyle karşılaştırılınca bazı avantajları ve dezavantajları bulunmaktadır. Bu noktada simetrik anahtar, şifrelerin yüksek veri oranlarına sahip olacak şekilde tasarlanarak saniyede megabayt'lık şifreleme ya da yazılım uygulamalarına ulaşabilmesi, simetrik şifreleme anahtarlarının nispeten daha kısa olması, güçlü şifreler üretmeye uygun olması, analiz edilmesi kolay olan basit dönüşümlerin güçlü ürün şifrelerini oluşturmak için kullanılabilmesi simetrik şifrelemenin avantajlı yönleri arasında değerlendirilmektedir. Ancak bu avantajlara ek olarak iki taraflı bir iletişimin gerçekleşebilmesi için anahtarın, gönderen ve alıcı tarafından paylaşılmasının zorunlu olması ve büyük bir ağda yönetilmesi gereken en fazla (n. (n-1))/ 2 anahtar çiftinin olması gibi dezavantajları da bulunmaktadır (Yadav, 2010: 10-11).

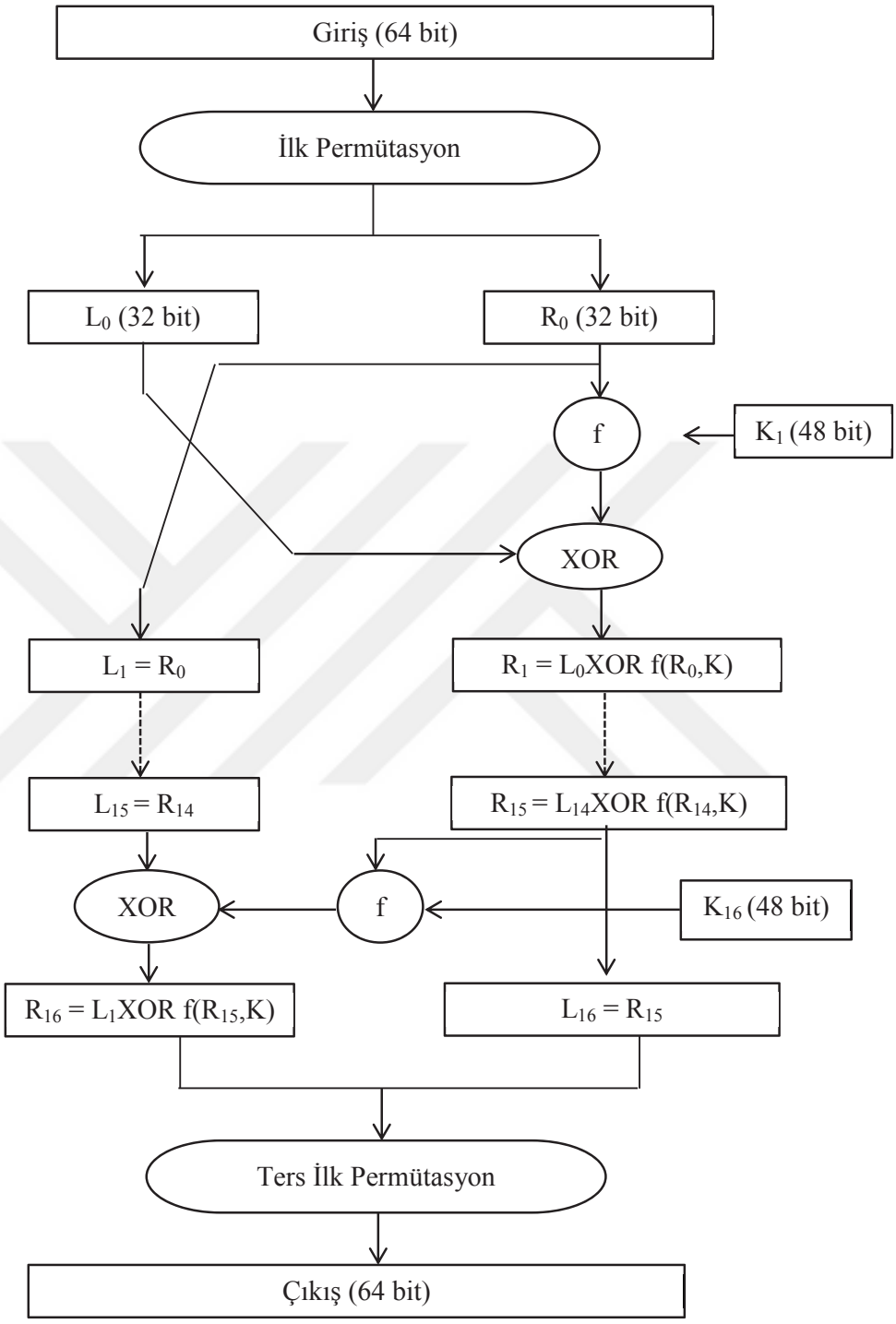
Simetrik şifreleme yönteminde şifreleme ile şifre çözme anahtarının aynı olması anahtar dağıtımının, bilginin iletilmesinden önce gerçekleştirilmesine neden olmuştur. Bu özelliği simetrik şifrelemenin, kriptografi biliminde önemli bir rol

oynamasına neden olmuş ve bu yönde farklı türde simetrik şifreleme türleri de kendini göstermiştir. Bu yönde en yaygın simetrik şifreleme türleri DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard), RC2 (Rivest Cipher), ve son olarak BLOWFISH olarak sıralanmaktadır. Çalışmanın bundan sonraki kısmında simetrik şifrelemenin bu türleri ayrıntılı bir şekilde açıklanmıştır (Agrawal ve Mishra, 2012: 878).

1. 6. 3. 1. 2. 1. DES Simetrik Şifreleme Algoritması

DES (Data Encryption Standard), bir blok şifresidir ve her biri 64 bit büyüklüğünde olan bloktaki verileri şifrelemektedir. Simetrik şifreleme türü olarak aynı algoritma ve anahtarı (K), anahtar kısmının ters çevrilmesi gibi küçük bir farkla birlikte, hem şifreleme hem de şifre çözme işlemi için kullanmaktadır. Anahtar uzunluğu ise 56 bittir. DES anahtar üretiminde ilk anahtar 64 bitten oluşmaktadır. Ancak DES işlemi başlamadan önce, anahtarın her 8 bit'i 56 bit anahtar üretmek için ayrılmaktadır. DES yönteminde şifreleme her biri round (döngü) sayılan 16 adımdan oluşmaktadır. İlk adımda ise 64 bitlik düzmetin bloğu ile ilk permütasyon (IP) işlevini gerçekleştirmektedir. İlk permütasyon düzmetin üzerinden gerçekleştikten sonra sol düz metin (LPT) ve sağ düz metin (RPT) üretilmektedir. Daha sonra ise LPT ve RPT şifreleme işlemi için 16 rounds gerçekleştirmektedir. Bu işlemlerin sonunda ise sol ve sağ düzmetin birleştirilerek işlemin sonunda 64 bitlik şifre metni oluşturulmaktadır (Kumar, Munjal ve Sharma, 2011: 62).

Bu aşamalar teorik olarak kısmen karışık görünsense bile bunu daha kolay ve anlaşılır hale getirmek için matematiksel bir model halinde bir şekil oluşturulmuş ve böylelikle yapılan bu açıklamaların net bir şekilde görülmesi sağlanmıştır. Bu anlaşılabilirliği kolaştıran şema ise Şekil 11'de gösterilmiştir.

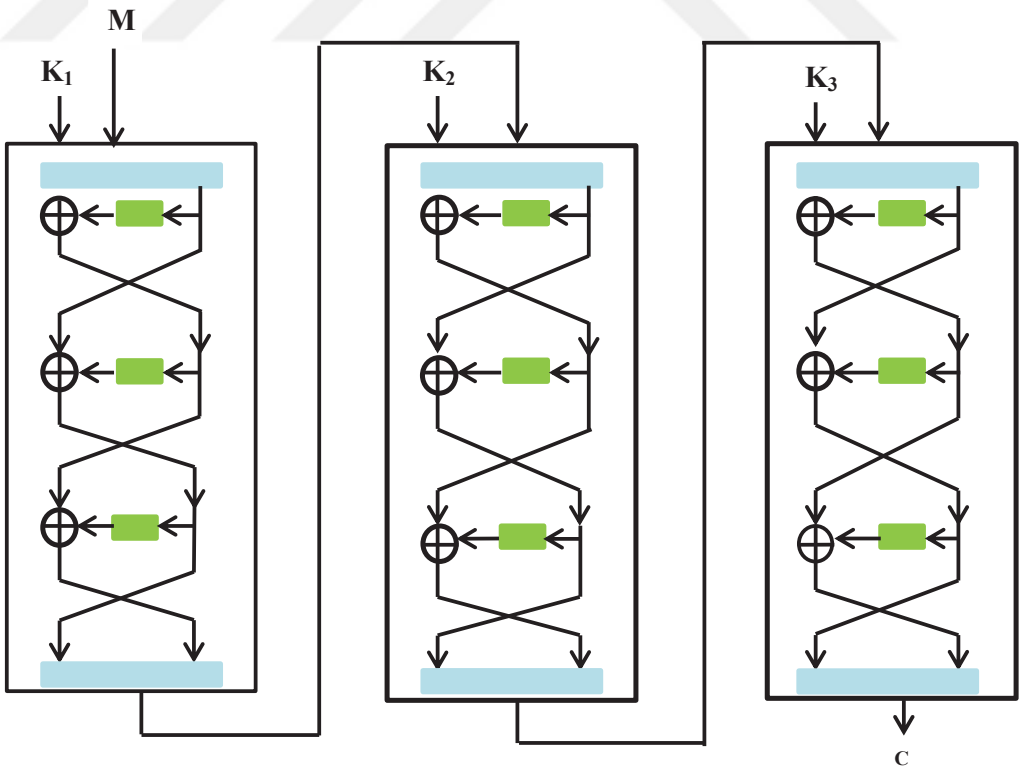


Kaynak: (Mahajan ve Sachdeva, 2013: 16).

Şekil 11: DES Algoritma Diyagramı

1. 6. 3. 1. 2. 2. 3DES Şifreleme Yöntemi

3DES şifreleme algoritması DES şifreleme yöntemindeki belirgin kusurları ele almak için geliştirilmiştir. DES şifreleme yönteminin kullandığı 56 bitlik bir anahtar hassas verileri şifrelemek için yeterli olmamıştır. Bu noktada 3DES şifreleme yöntemiyle bu kusurun giderilmesi amaçlanmış ve DES algoritmasının art arda 3 kere çalıştırılması ile oluşturularak DES'in anahtar boyutu genişletilmiştir. Bu şekilde anahtar büyüklüğü 168 bit (3 x 56 bit) olmuştur ve K1, K2 ve K3 olmak üzere 3 farklı anahtar kullanılmıştır. Burada ilk olarak düzmetin, K1 anahtarıyla daha sonra K2 ve en sonda K3 anahtarıyla şifrelenmektedir. Ancak 3DES yönteminin bu şekilde 3 kere art arda çalıştırılması sistemin DES yöntemiyle kıyaslandığında 3 kat daha yavaş işlemesine ve dolayısıyla şifreleme süresinin uzamasına neden olmuştur. (Singh ve Supriya, 2013: 35). Bu şekilde işleyen 3DES yönteminin akış şeması Şekil 12'de gösterilmiştir.



Kaynak: (Yılmaz, 2017: 26).

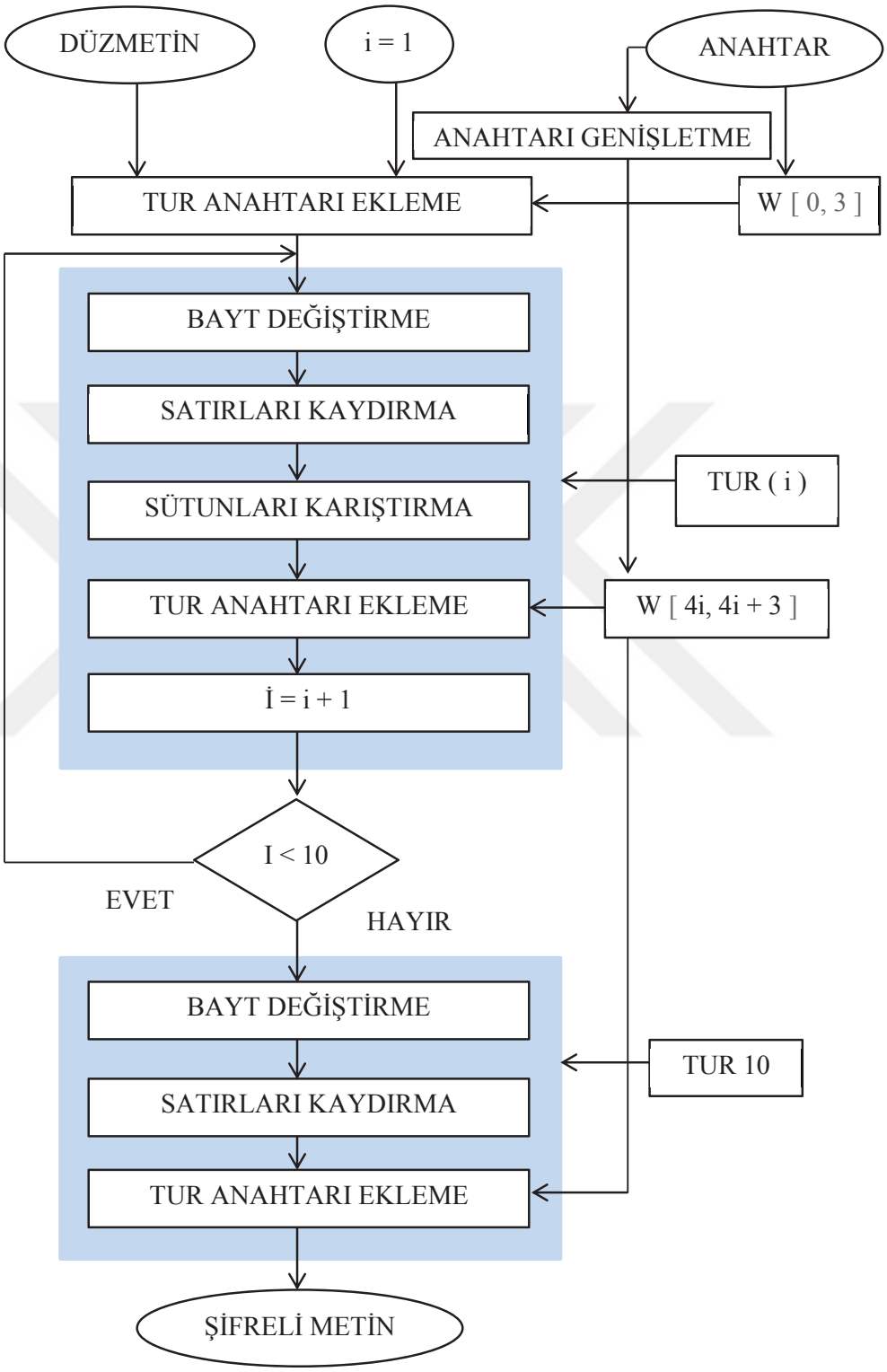
Şekil 12: 3DES Algoritması Akış Şeması

3DES algoritmanın diğer bir önemli özelliği ise 3 kez çalıştırılmakla birlikte iki anahtar kullanılarak üçlü şifreleme yapmasıdır. Bu şekilde DES yöntemine göre güvenlik seviyesini 2 katına çıkarmaktadır. Bu 112 bitlik bir anahtara denk gelmekte ve güvenlik şifreleme işlemi boyunca tamamen orantılı bir şekilde artmaktadır. DES şifreleme yönteminin aksine şifreleme için 24 bayt'lık anahtarlar kullanmaktadır. Bu şekilde veriler, anahtarın ilk 8 bayt'ını kullanarak şifrelenmekte, anahtarın ortasında ise 8 bay'ını daha kullanarak deşifreleme işlemi gerçekleştirilmektedir. Anahtarın son 8 bayt'lık kısmıyle ise şifreleme yapılıp tekrar 8 bayt'lık veri oluşturmak için kullanılmaktadır (Şahin, 2015: 35-36).

Bu özellikler 3DES algoritmasının, diğer algoritmalarla kıyaslandığı zaman, bazı avantajlarını ortaya çıkarmaktadır. Bu doğrultuda uygulanması oldukça kolaydır ve güvenliği sağlayarak verilerin kolay bir şekilde saklanması neden olmaktadır. Özellikle finansal sistemlerde ve elektronik pasaportlarda biometrik bilgilerin korunmasında oldukça yaygın kullanılmaktadır. Ancak bu avantajların yanı sıra her şifreleme algoritmasında olduğu gibi kendi içerisinde bazı dezavantajlar da bulundurmaktadır. Örneğin iki bağımsız anahtarlı 3DES algoritması için, toplam anahtar uzunluğu yeterli olmayarak 112 bit'e düşürülebilmektedir. Bu güvenlik açığı, hackerlara bir anahtarı alma ve uzunluğunu azaltma fırsatı vermekte ve anahtarı kırmak için gerekli süreyi azaltarak başka bir güvenlik açığına neden olmaktadır. Aynı zamanda daha ağır bir şekilde işlemesi de 3DES algoritması için bir dezavantaj olarak değerlendirilmektedir (Aleisa, 2015: 244).

1. 6. 3. 1. 2. 3. AES Kriptoloji Algoritması

AES, blok uzunluğu 128 bit olan bir blok şifre türüdür. AES 128, 192 ve 256 bit olmak üzere üç farklı anahtar uzunluğuna olanak vermektedir. Şifreleme işleminde 128 bitlik anahtar için 10 round (tur), 192 bitlik anahtar için 12 tur ve son olarak 256 bit'lik anahtar için 14 tur oluşmaktadır. DES' den farklı olarak şifre çözme algoritması önemli ölçüde farklıdır. Genel olarak aynı adımlar şifreleme ve şifre çözme işlemleri için kullanılsa da adımların uygulanma sırası farklılık göstermektedir (Rihan, Khalid ve Osman, 2015: 152). Bu doğrultuda AES işlem süreci Şekil 13'de gösterilmiştir.



Kaynak: (Singh ve Supriya, 2013: 36).

Şekil 13: AES İşlem Süreci

AES şifreleme algoritmasında işlem sürecinin gerçekleştirilebilmesi için Şekil 13'de gösterilen bayt değiştirme, satırları kaydırma, sütunları karıştırma ve tur anahtarının değiştirilmesi gibi aşamaların gerçekleşmesi gerekmektedir. Bu tur dönüşüm işlemleri aşağıda ayrıntılı bir şekilde açıklanmıştır.

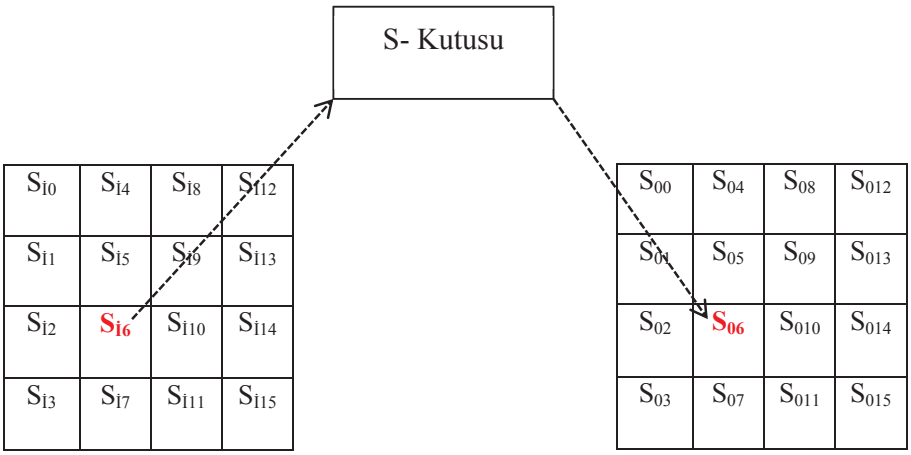
I. Bayt Değiştirme: Bayt yer değiştirme işlemi, algoritmada bulunan tek doğrusal olmayan dönüşümdür. Bayt değiştirme dönüşümü, girişindeki durumun her bir bayt'ını (S-Box) çıkış tablosu denilen bir değiştirme tablosu kullanarak, başka bir bayt'a dönüştürmektedir. (S-Box) çıkış tablosu Tablo 5'te gösterilmiştir (Başkök, 2007: 78).

Tablo 5: (S-Box) Çıkış Tablosu

	x0	**x1**	**x2**	**x3**	**x4**	**x5**	**x6**	**x7**	**x8**	**x9**	**xa**	**xb**	**xc**	**xd**	**xe**	**xf**
ox	63	7c	77	7b	f2	6b	df	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Kaynak: (Öztemür, 2012: 28).

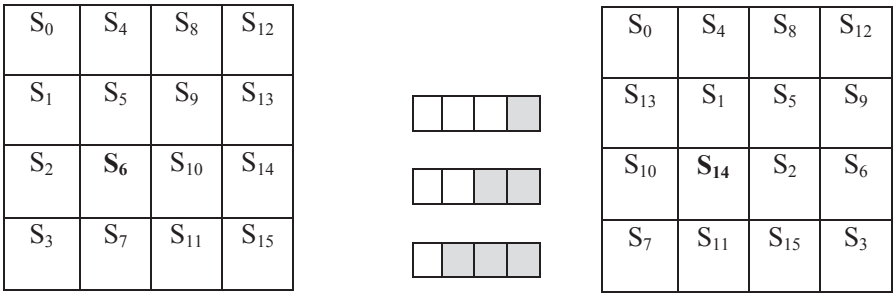
Burada ilk olarak 128 bitlik veriler 8'er bitlik 16 parçaya ayrılmakta ve 4x4 boyutunda olan bir durum matrisi oluşturulmaktadır. Tüm işlemler bahsedilen durum matrisi üzerinden gerçekleştirilmektedir. Diğer yandan bayt değiştirme adımında her 8 bitlik paraçaya matematiksel dönüşüm işlemi gerçekleştirilmektedir. Bu dönüşüm ise iki aşamada gerçekleştirilerek ilk aşamada indirgeme polinomu $P(x) = x^8 + x^4 + x^3 + x + 1$ kullanılarak çarpmaya göre tersi alınmaktadır. Buradan elde edilen sonuçlar ise geçiş matrisi ile çarpılarak sabit bir matris toplanılmaktadır. Bu şekilde işlem gerçekleştirilmiş olmaktadır (Kula, 2009: 12). Bu süreç Şekil 14'te gösterilmiştir.



Kaynak: (Öztemür, 2012: 29).

Şekil 14: Bayt Değiştirme İşlemi

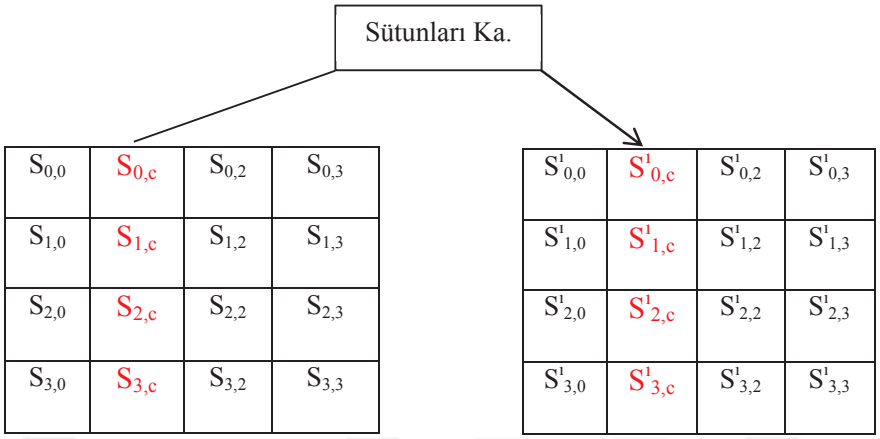
II. Satırları Kaydırma: Satırları kaydırma işleminde durum matrisinin ilk satırı dışında diğer satırların tamamında kaydırma işlemi yapılmaktadır. Bu kaydırma işlemi gerçekleştirilirken de ikinci satır 1 bayt, üçüncü satır 2 bayt ve son satır 3 bayt kaydırılmaktadır. Satır Kaydırma İşlemi Şekil 15'te gösterilmiştir (Eriş ve Kaya, 2016: 117).



Kaynak: (Başkök, 2007: 83).

Şekil 15: Satırları Kaydırma Katmanı

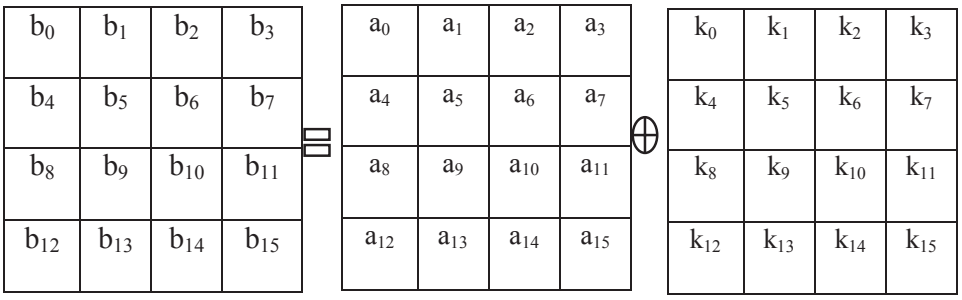
III. Sütunları Karıştırma: Durum matrisinde yer alan her bir sütun üzerinde bağımsız bir şekilde gerçekleşmektedir. Her bir satırın polinom olarak düşünülmesiyle a (x) = { 03 } $\mathbf{x^3}$ + { 01} x^2 + { 01} x + { 02} polinomu ile x^4+ 2 modülü arasında çarpma işlemi gerçekleştirilmektedir. Sütunları karıştırma işlemi Şekil 16'de gösterilmiştir (Doğan, 2008: 34).



Kaynak: (Kula, 2009: 14).

Şekil 16: Sütunları Karıştırma İşlemi

IV. Tur Anahtarı Ekleme: Tur dönüşüm işlemlerinin sonuncusu, sütunları karıştırma işleminden sonra gerçekleştirilen tur anahtarı ekleme işlemidir. Burada hem şifreleme yapılmasında hem de yapılan şifrenin çözülmesinde aynı dönüşüm kullanılmaktadır. Dönüşümün tersi de kendisine eşittir. Sütunları karıştırma işleminden sonra elde edilen matris ile 128 bitlik tur anahtarı matrisinin "xor" lanmasıyla elde edilmektedir. Tur anahtarı ekleme işlemi Şekil 17'da gösterilmiştir (Büyükkaya, 2017: 27).

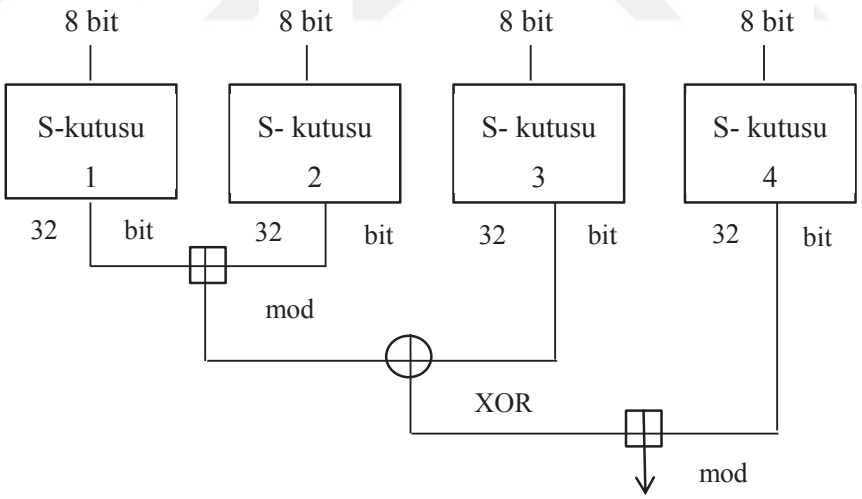


Kaynak: (Başkök, 2007: 86).

Şekil 17: Tur Anahtarı Ekleme Katmanı

1. 6. 3. 1. 2. 4. Blowfish Simetrik Şifreleme Yöntemi

Blowfish, verilerin şifrelenmesinde ve korunmasında etkili bir şekilde kullanılan simetrik bir blok şifreleme yöntemidir. 64 bitlik blok boyutu bulunup 32 bit'ten 448 bit'e kadar değişken uzunlukta bir anahtara sahip olabilirken veri güvenliğini sağlamak için oldukça uygun bir yapıda bulunmaktadır. Bugün şifreleme algoritmalarının çoğu halka açık değildir ve bunların çoğu patentler ya da hükümetler tarafından korunmaktadır. Blowfish algoritması da yeni bir şifreleme algoritması sağlamak için, dünyanın önde gelen kriptograflarından olan Bruce Schneier tarafından 1993 yılında tasarlanarak kamuya açık hale getirilmiştir. Dolayısıyla Blowfish patentsiz ve lisanssız olup tüm kullanımlar için ücretsiz olarak kullanılabilmektedir. Diğer yandan tasarımında mevcut şifreleme algoritmalarına hızlı ve ücretsiz bir alternatif sağlamak amacıyla hareket edilmiştir (Thakur ve Kumar, 2011: 9). Blowfish şifreleme yönteminin işleyişi Şekil 18'de gösterilmiştir.



Kaynak: (Bhanot ve Hans, 2015: 298).

Şekil 18: Blowfish Fonksiyon Akış Şeması

1. 6. 3. 1. 2. 5. RC2 Algoritması

1987 yılında RSA güvenlik şirketi için Ron Rivest tarafından tasarlanmıştır. RC simge olarak "Rivest Cipher" ı simgelemektedir. Ancak bu simgenin "Ron's

Code" u simgelendiği de literatürde düşünülmektedir. DES algoritmasının yerine geçmesi düşüncesiyle tasarlamıştır. DES algoritmasından ise yaklaşık 3 kat daha hızlı çalışmaktadır. Genel olarak 64 bitlik bir anahtara sahip olmasına rağmen ihtiyaç duyulduğu zamanlarda 40-88 bit aralığında bir uzunluğa sahip anahtar, ek olarak, kullanılabilmektedir (Aslanyürek, 2018: 18).

Çalışmanın bu bölümüne kadar simetrik şifreleme yöntemlerinin başlıca türleri olan DES, 3DES AES, Blowfish ve RC2 algoritmaları ayrıntılı bir şekilde açıklanmıştır. Bu bağlamda bu türler arasındaki farklılıkların net olarak görülebilmesi için bir tablo oluşturulmuş ve bu tablo Tablo 6'da gösterilmiştir.

Tablo 6: Simetrik Şifreleme Türlerinin Karşılaştırılması

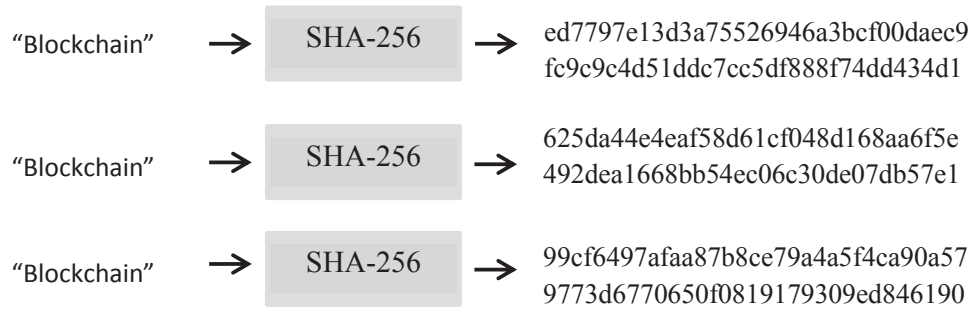
Algoritma	Blok Uzunluğu	Anahtar Uzunluğu	Döngü (Tur) Sayısı
DES	64 bit	56 bit	16
3DES	64 bit	168 bit	48
AES	128 bit	128, 192 veya 256 bit	10, 12, 14
Blowfish	64 bit	448 bit'e kadar	16
RC2	-	2048 bit'e kadar	Bilinmiyor

Kaynak: (Patil ve Goudar, 2013: 64; Kodaz ve Botsalı, 2010: 13).

1. 6. 3. 1. 3. Hash (Özet, Karmalama) ve SHA-256

Blockchain teknolojisinin güvenilirliği ve bütünlüğü; çift harcama, hatalı erişim, kayıt altına alınmama gibi bir durum söz konusu olmadığı için hashing sistemine bağlı olarak çalışmaktadır. Hash sistemi, güvenilirliği temin etmedeki en önemli unsuru hatta kilit noktasını oluşturmaktadır. Hash'in yani karmalamanın özelliği herhangi uzunluktaki bir girdiyi alarak bu girdinin matematiksel algoritmalar aracılığıyla şifreli sabit bir çıktıya dönüştürmesidir. Girdiyi oluşturan veriler, bir mesaj ya da bir işlem bloğu hatta internette yer alan tüm veriler gibi büyük bir önbellekten oluşabileceği gibi bunlar aynı zamanda kısa bilgi parçalarını da bünyesinde bulundurabilmektedir. Hash, verilerin güvenliğini büyük bir oranda artırmaktadır. Çünkü şifrelenmiş bilginin uzunluğu hesaplanamayacağı gibi verilerin şifrelere bakılarak çözülebilmesini imkânsız hale getirmektedir (Atabaş, 2018: 30-31).

Hash fonksiyonu, farklı uzunluktaki verilerden sabit uzunluktaki verilerin özetini çıkarmaktadır. Bundan dolayı özet fonksiyonu olarak da isimlendirilmektedir. Burada önemli olan özet fonksiyondan hareket edilerek özetlenen veri hakkında çeşitli bilgiler üretilememesine dikkat edilmesi gerektiğidir. Yani özet verilerin ya da mesajların rastgele oluşturulmuş gibi bir izlenim oluşturması gerekmektedir. Bu sistem sayesin blokzincir Hash fonksiyonunu fazla kullanmakta ve blockchain'in temelini oluşturmaktadır. Bu bağlamda Bitcoin işlemlerinde SHA-256 isimli hash fonksiyonunu kullanmaktadır. SHA-256 özet fonksiyonunda, mesajın uzunluğuna bakılmaksızın, 256 bit (32 byte) mesaj oluşturulmaktadır. Diğer bir ifadeyle SHA-256 fonksiyonu, veri girdisi ne olursa olsun, verinin özeti 256 tane ardışık 0 ya da 1' den oluşan bir dizeden oluşmaktadır. Okumanın kolay olması için de genel olarak dörtlü gruplar halinde ve 16'lık sistem ile yazılmaktadırlar. Veri özetleri yaklaşık 64 adet (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) harfleri kullanılarak yazılmaktadır. Bu durumda SHA-256 fonksiyonunda 256 tane ardışık 0 ve 1 sayılarıyla toplamda $2^{256} \approx 1.15 \text{ X } 10^{77}$ tane farklı ve büyük sayıda özet elde edilebilmektedir (Çarkacıoğlu, 2016: 21-22). SHA-256 özet fonksiyonun örneği Şekil 19'de gösterilmiştir.



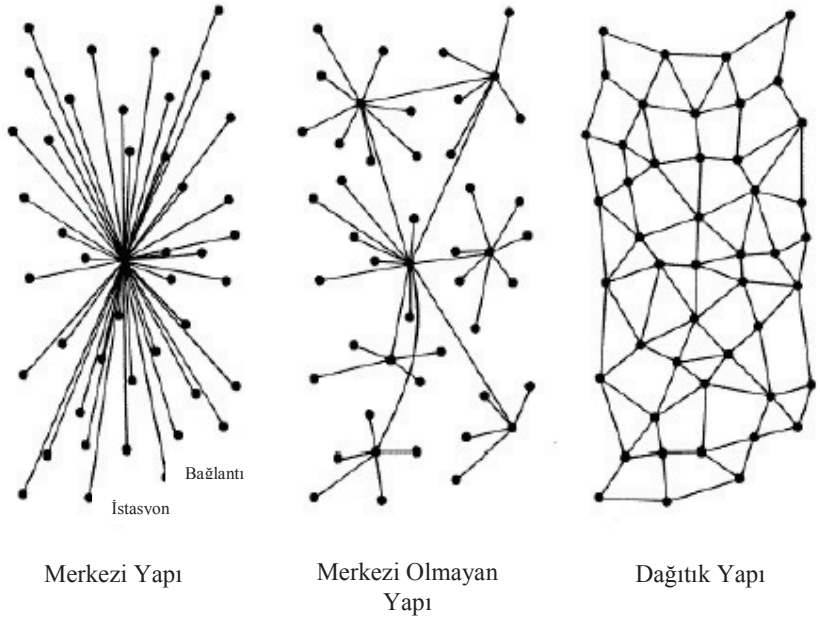
Kaynak: (Gündüz ve Tepeci, 2018: 44).

Şekil 19: SHA-256 Hash Algoritması Çıktı Örneği

1. 6. 3. 2. Dağıtık Bir Ağ Yapısı

Blockchain, birden çok kullanıcı arasında eşler arası (Peer to peer - P2P) işlem yapılmasına olanak sağlayan bir teknoloji yapısına sahip olup sistemin güvenli

bir şekilde işlemesinde önemli bir rol oynamaktadır. Blokzincir güvenliği ise tek bir unsura bağlı olarak değil birden çok faktörün bir araya getirilmesiyle oluşturulmaktadır. Bunlar kriptoloji, mutabakat, doğrulama mekanizması ve dağıtık defter kaydı gibi faktörlerdir. Burada dağıtık defter teknolojisi (Distributed Ledger Tecknolohy-DLT) blokzincir ağındaki verilerin bir yerlerde depolanma zorunluluğundan oluşturulmaktadır. Ancak dağıtık ağ yapısı merkezi ve çok merkezli ağ yapılarından farklı özellikler sergilemektedir. Bu farklılıklar Şekil 20'da net bir şekilde görülmektedir (Aktaş, 2018: 21).



Kaynak: (Baran, 1964: 2).

Şekil 20: Merkezi, Merkezi Olmayan ve Dağıtık Yapı Arasındaki Fark

Merkezi yapılarda, veriler tek bir merkezde tutularak bilgiyi değiştirme ya da silme gibi yetkinin tamamı sadece merkeze aittir. Bu durum sistemin tek bir kontrol merkezi tarafından yönetilmesine olanak sağlamakta ancak bu işleyiş beraberinde bir dezavantajı da getirmektedir. Çünkü tek bir merkeze bağlılık bu merkezde meydana gelecek ciddi bir sorunun tüm sistemi altüst etmesine neden olabilmektedir. Çok merkezli yani merkezi olmayan yapılar ise ağ üzerindeki kullanıcıların birbirleriyle iletişim kurma yöntemlerine dayanmaktadır. Bu şekilde düğümler arasındaki

bağlantılar yönetilebilmektedir. Merkezi ve merkezi olmayan yapıların bu özelliklerine bakılınca blokzincir, bu yapılarda yaşanabilecek mevcut olumsuzlukları ortadan kaldırabilmek için, dağıtık bir sistem yapısını bünyesinde bulunmaktadır. Blokzincir'i geleneksel veri tabanlarından ayıran en önemli özellikte budur (Aldemir, 2018: 12).

Blokzincir teknolojisinin bünyesinde bulundurduğu DLT, diğer sistemler ile kıyaslandığında büyük olan bir ağ içerisindeki tüm katılımcılar tarafından tutulan ve güncelleştirilmiş bir veri tabanıdır. Dolayısıyla dağıtım işlemleri benzersiz bir özellik sergilemektedir. Diğer sistemlerde olduğu gibi kayıtlar tek bir merkezden çeşitli düğümlere iletilmezler. Aksine zincire eklenen verilerin bir kopyası sisteme dâhil olarak pek çok bilgisayara eş zamanlı olarak kaydedilmekte ve ağ içerisindeki her bir düğüm, her işlemi işleyerek, kendi sonuçlarını ortaya çıkarmaktadır. En sonunda ise elde edilen bu sonuçların doğruluğu oy birliğiyle sağlanmaktadır. Dolayısıyla blockchain'in sahip olduğu dağıtık yapı sistemi bilgisayarların bazılarında bir sorun yaşansa bile blokzincirin güncel hali diğer bilgisayarlarda mevcut olduğu için herhangi bir kaybın yaşanmasının önüne geçmektedir. Aynı zamanda hackerların saldırıp verileri ele geçirme olasılığını ortadan kaldırmaktadır. Çünkü saldırının gerçekleşebilmesi için yüzbinlerce bilgisayarın yarısından çoğunun ele geçirilmesi gerekmektedir. Bu eylem teknik olarak %51 saldırısı (51% Attack) olarak adlandırılmaktadır. DLT' nin sahip olduğu bu özellikler sadece statik verilerde değil aynı zamanda dinamik verilerde de geçerlilik sağlamaktadır (Erözel Durbilmez ve Yılmaz Türkmen, 2019: 33).

1. 6. 3. 3. İşlem (Transaction) ve Blok Kavramı

Kripto paraya sahip olabilmek için içerisinde gizli ve açık olmak üzere iki adresin bulunduğu bir cüzdana sahip olunması gerekmektedir. Burada açık adres hesap numarası görevi görürken gizli adres şifre görevi görmekte ve birine kripto para gönderilmek istendiğinde kullanılmaktadır. Örneğin; A kişisi gizli adresi kullanarak, B kişisine göndereceği açık adresi yazarak transfer işlemini gerçekleştirmekte ve bu şekilde cüzdanda işlemler görülmektedir. Blockchain üzerinde kişinin sahip olduğu kripto paranın bakiyesi tutulmamakta dolayısıyla bir kişinin ne kadar kripto paraya sahip olduğunun anlaşılabilmesi için açık adresine gönderilenlere bakılması

gerekmektedir. Bir yere kripto para gönderilmek istendiğinde, karşı tarafın transfer edilmek istenen kripto para türüne sahip olup olmadığının anlaşılması bunun için de açık adrese gelen ve giden kripto para geçmişine bakılarak gönderilmek istenen kripto paranın hesapta var olup olmadığının doğrulanması gerekmektedir. Bu şekilde de işlem yaratılmış olmaktadır. Diğer yandan blokzincir ağında işlemler ağa yazılmadan önce madenciler tarafından, 2 kriterli doğrulama süreci dikkate alınarak, gerçekleştirilen işlemler kontrol edilmektedir. Burada ilk kriter işlem içerisindeki kripto paranın daha önceden kullanılıp kullanılmadığı; ikinci kriter ise işlemdeki imzanın doğruluğunun kontrol edilmesidir. Burada eğer doğru olduğu sonucuna ulaşılırsa işlemler onaylananlar havuzuna dâhil edilmekte ve zincire eklenmektedir. Bu şekilde de transaction işlemi onaylanmaktadır (Gündüz ve Tepeci, 2018: 45-46).

Blokzincir'de gerçekleştirilen her bir işlem belli yapıdaki bloklara kaydedilmektedir. Bundan dolayı blok kavramının ne olduğunun da iyi bilinmesi gerekmektedir. Bu bağlamda blok önceden gerçekleştirilmiş, bekleyen işlemleri onaylayarak bunların kayıtlarını tutan bir yapı olarak tanımlanmaktadır. Basit bir ifadeyle blok, hesap defterinin yeni bir sayfası olup her blok bir önceki bloğun üzerine eklenerek blokzinciri oluşturmaktadır. Yani bir blok dolunca verilerin Hash'i (daha küçük ve rastgele sıralanmış harfler ve rakamlar) oluşturulmakta ve bunun üzerine yeni bir blok eklenmektedir. En son eklenen bloğun girdilerinden biri, bir önceki bloğun Hash değeridir ve blok zincirin oluşmasına neden olan unsur da bu şekilde blokların bir zincir gibi üst üste eklenmesidir. Bu durum her bloğun bir önceki bloğa bağlı olarak şifrelenmesine neden olup blokta bir değişiklik meydana gelmesi için bir önceki blokta da değişikler yapılmasını zorunlu kılmaktadır (Abaday, 2018: 45-46).

2009 yılında ağda oluşan ilk blok "Genesis Blok" olup bu ilk bloktan sonra farklı bloklarda yer alan bir işlem zinciri oluşmuştur. Bloklarda gerçekleştirilen her bir işlem ilk blok olan Genesis Blok'a kadar geriye doğru takip edilebilmektedir. Ancak bir bloğa bağlı birden fazla blok olmaması gerekmektedir. Aksi takdirde çatallaşma (forking) adı verilen bir durum meydana gelmektedir. Diğer yandan Genesis Bloğunda, bir önceki bloğun Hash değerine sahip bir blok söz konusu olmadığından dolayı zincirin yaratıcısı tarafından bir değer atanmakta ve bu değerler genellikle 256 tane 0'dan oluşmaktadır. Aynı zamanda birbirinin ardına dizilen zincir bloklarından bir önceki bloğa "parent block- ebeveyn blok" denilmekte ve her bloğun yalnızca bir parent block'u olmaktadır. Ancak her bloğun yalnızca bir adet parent

block'u olabileceği gibi her parent block'undan yalnızca bir adet "child block" olarak isimlendirilen yavru bloğunun olabileceğinin de bilinmesi gerekmektedir (Güven ve Şahinöz, 2018: 53-54).

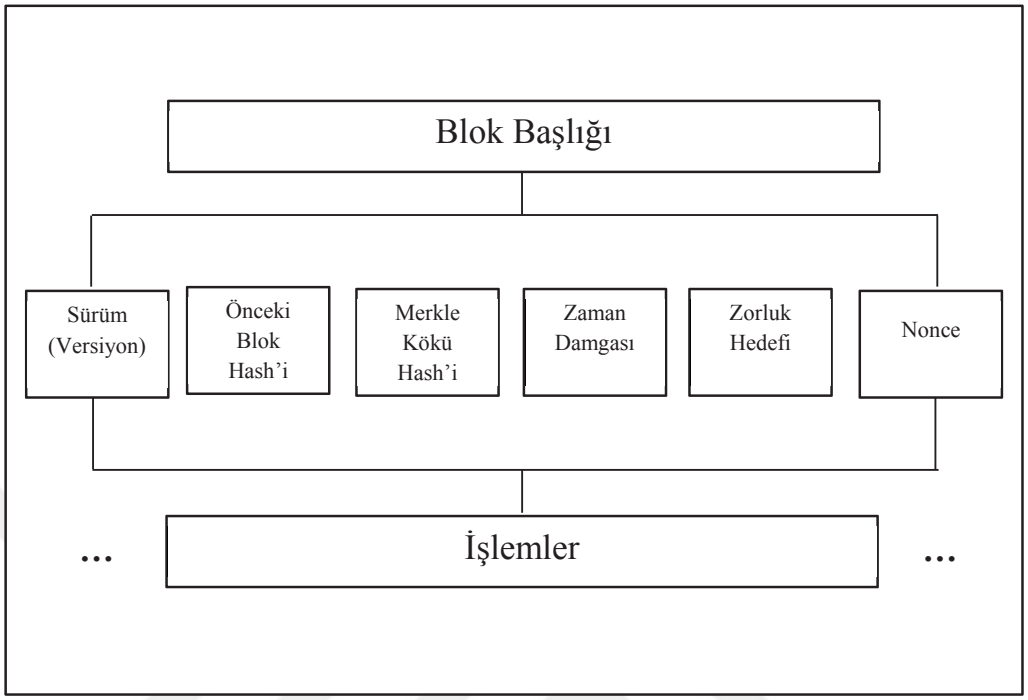
Bu şekilde eşsiz bir yapıya sahip olan blokzincirdeki bir blok onu diğerlerinden benzersiz bir şekilde tanımlayan bir formata sahiptir. Bu formdaki ilk oluşum sihirli sayıdır. Sihirli sayıyı blok boyut takip etmektedir. Blok boyutundan sonraki yapı ise blok başlığıdır. Blok başlığı Bitcoin başlıklarında yapıldığı gibi SHA-256 ile birleştirilmiştir ve blok zincir ağındaki değişmezliğin sağlanması açısından çok önemli bir rol oynamaktadır. Çünkü bir hacker bir blok başlığını değiştirmek istediğinde bloğun başlığını tahrif etmek için ilk blok olan Genesis Bloğundan başlayarak tüm blok başlıklarını değiştirmesi gerekmektedir. Bu durum da ağda daha yüksek bir güvenlik seviyesinin sağlanmasına neden olmaktadır. Blok formatını başlık kayıtlarından sonra kaç tane işlem yapıldığını gösteren kayıt sayacı ve kayıtlar takip etmektedir (Gao vd., 2018: 9922). Bu şekilde işleyen bir blok yapısı Tablo 7'de net bir şekilde gösterilmiştir.

Tablo 7: Blockchain ve Blok Yapısı

Alan Adı	Boyut	Açıklama
Sihirli Sayı	4 Byte	"Aşağıdaki bir bloktur." Anlamındadır. Sihirli sayı her zaman 0Xd0b4bef9' dur.
Blok Boyutu	4 Byte	Bloğun büyüklüğünü göstermektedir.
Blok Başlığı	80 Byte	Çeşitli alanlardan oluşmaktadır.
Kayıt Sayacı	1-9 Byte	Kaç adet kayıt olduğunu göstermektedir.
Kayıtlar	Değişir	Kaydedilen işlemlerdir.

Kaynak: (Güven ve Şahinöz, 2018: 54).

Bir blok başlığının güvenlik açısından önemi yukarıda açıklanmıştır. Bu bağlamda blok başlığının da ayrıntılı bir şekilde açıklanması büyük bir önem arz etmektedir. Bir blok başlığında; bir önceki blok başlığının şifreli özet değeri, merkle kök özeti, zorluk derecesi ve sürüm gibi içerisinde çeşitli kavramlar bulunmakta ve Şekil 21'da gösterilen 6 farklı alt alan bulunmaktadır (Kardaş ve Kiraz, 2018: 4).



Kaynak: Yazar Tarafından Oluşturulmuştur.

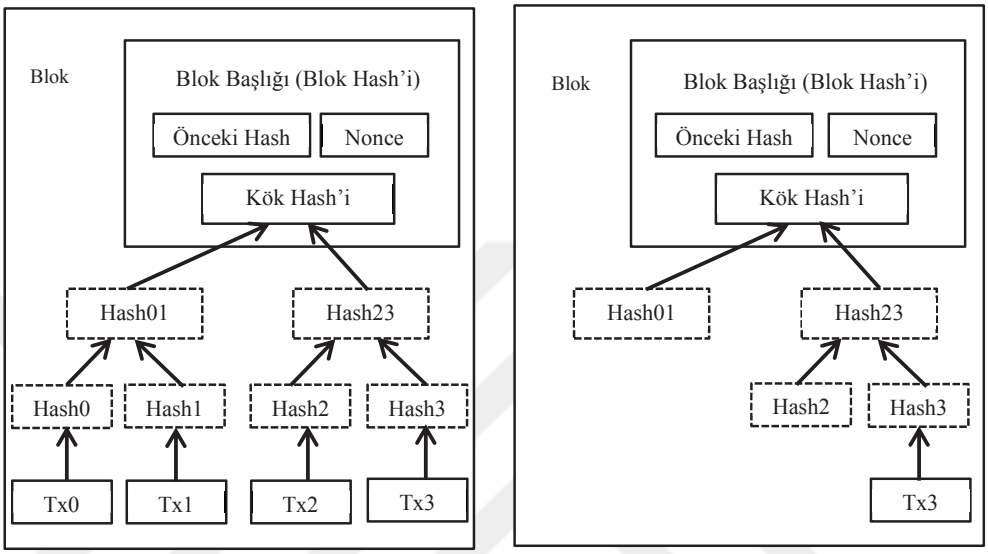
Şekil 21: Blok Başlığı Alt Türleri

I. Sürüm (Versiyon): Bloğun sürüm boyutu 4 Byte olmakla birlikte bir blok oluşturulurken gerek yapısı gerek uzunluğu gibi sağlaması gereken bazı kurallar bulunmaktadır. Bir bloğun versiyonu, hangi blok doğrulama kurallarının uygulanacağını göstermektedir (Tanrıverdi, Uysal ve Üstündağ, 2019: 207).

II. Önceki Blok Hash'i: Blokchain'de her bir blok birbirlerine zincirler halinde eklenmektedir. Bu bloklar da birbirlerine Hash değeri üzerinden bağlanmaktadır. Dolayısıyla bu kavram bir önceki bloğun Hash değerini temsil etmektedir (Özcan, 2019: 10).

III. Merkle Kökü Hash'i: Bir merkle ağacı çok sayıda verinin bir araya getirilmesine ve bu veri yığınlarının doğrulanmasına olanak sağlamaktadır. Merke ağacında işlemlerin gerçekleştirildiği her bir blok içerisinde tüm işlemler ikişerli gruplar halinde özetlenmektedir. Bu işlemin sonunda ortaya çıkan özetler ise tekrardan kendi aralarında ikişerli gruplar halinde özetlenmekte ve bu süreç sürekli olarak bu şekilde devam etmektedir. Bu işlem ancak tek bir özet elde edildiği zaman sonlandırılmaktadır. Bu işlem sonucunda işlemleri ikişerli olarak özetlenmesinden

oluşan ağaç yapısına merkle ağacı ve işleminin devam etmesiyle elde edilen nihai tek özete ise merkle kökü denilmektedir (Şen, 2019: 90). Merkle ağaç Hash işlem yapısı Şekil 22'de gösterilmiştir.



Kaynak: (Nakamoto, 2008: 4)

Şekil 22: Merkle Ağacında Hash İşlemi ve Tx0-2 Budanmış Merkle Ağacı

Merkle ağacı SPV (Simplified Payment Verification) yani Basitleştirilmiş Ödeme Doğrulama olarak bilinen bir protokol tarafından kullanılmaktadır. Bu tür protokoller tüm blokları indirmezken işlem teyidi için sadece blok başlıklarını indirerek merkle ağacını kontrol etmektedirler. Merkle ağaç sisteminin bu şekilde işlemesindeki avantaj, eğer kötü niyetli bir kullanıcı sahte bir işlemle bir merkle ağacının dibine takas etmeye çalışırsa, meydana gelecek değişiklikler yukarıda yer alan düğümlerde bir değişikliğe neden olarak protokolün onu tamamen farklı bir blok olarak kaydetmesine sebep olmaktadır (Buterin, 2014: 9-10).

IV. Zaman Damgası: Bloğun oluşturulduğu zamanı göstermektedir. Blok oluşturulurken bir bloğa eklenen 4 Byte'lık bir boyuta sahip zaman bilgisini temsil etmektedir (Kösesoy, 2019: 6).

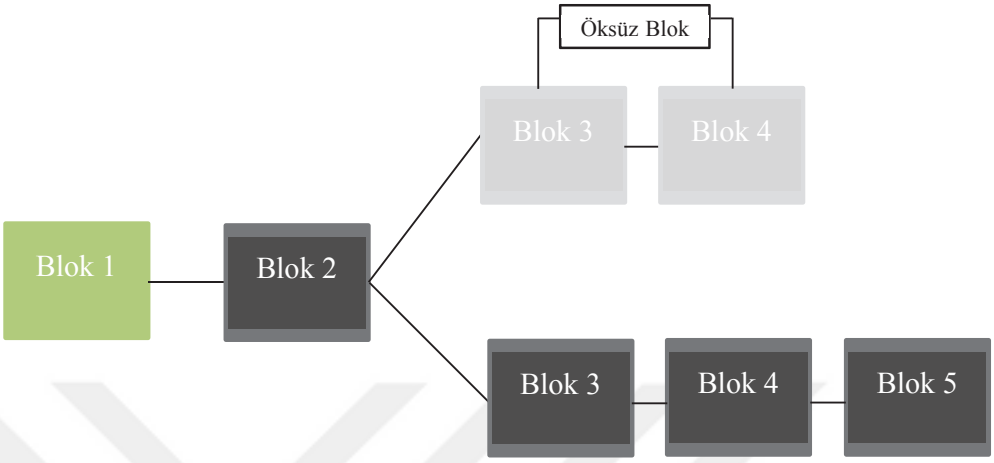
V. Zorluk Hedefi: Zorluk, bir bloğun sahip olduğu Hash değerinin ortaya çıkması için gereken sürenin azaltılıp artırılmasına yarayan bir parametredir. Burada

yeni bir madenci ağa katıldığı zaman blok oluşma süresinin kısalmamasını istemekte ve bundan dolayı bu değeri artırmaktadır. Tam tersi ağda bulunan bir madencinin bu ağ içerisinden çıktığı zaman ise değeri azaltılmaktadır. Böylelikle blok oluşturulma süresi sabit bir seviyede tutulmaktadır. Çünkü blokların ortalama 10 dakikada bir oluşturulması hedeflenmektedir (Özcan, 2019: 10).

VI. Nonce: Blok başlığı bir nonce içermektedir ve madenciler de farklı Hash değerleri elde etmek için nonce'ı sık sık değiştirmektedir. Bu bağlamda nonce, blok içerisindeki en uygun Hash değerini bulabilmek için madenciler tarafından algoritmanın kaç kere çalıştırıldığının görülmesi açısından önemli bir kavram olarak değerlendirilmektedir. Nonce her Hash hesaplama işlemi için 4 Byte'lık bir alan boyutuna sahiptir (Zheng vd., 2017: 558-560).

1. 6. 3. 4. Orphan (Öksüz) Blok

Blockchain ağında normalde bir bloğa yalnızca bir blok eklenmekte ve bu şekilde zincir oluşturularak süreç devam etmektedir. Bu şekilde iş ispatı yapan ve blok bulan madenciye zincire eklediği blok için ödül verilmektedir. Ancak bazı durumlarda birden fazla madenci aynı zamanlı olarak iş ispatı yapmakta ve buldukları blokları blokzincire eklemektedirler. Bu durum sistemin işleyişinde aksaklıklara neden olmayacak çünkü iki farklı blok zincire eklenemeyeceğinden dolayı zincirlerden biri sistemde varlığını sürdürmeye devam ederken bir diğeri sistem tarafından dışlanmaktadır. Ancak burada her bir tam uç farklı bloğu doğru kabul edeceğinden dolayı çatallaşma meydana gelmektedir. Uzun vadede ise uçlar çatalın en uzun olan ucunu doğru kabul ederken diğer uçtaki bloklar dışlanarak öksüz blok olarak adlandırılmaktadır. (Çarkacıoğlu, 2016: 44-45). Orphan Blok Örneği Şekil 23'de gösterilmiştir.



Kaynak: (Scherer, 2017: 8).

Şekil 23: Orphan (Öksüz) Blok Örneği

Günde ortalama olarak 3 defa öksüz blok olayı gerçekleşmektedir ve bu orphan bloğun yüzde olarak gerçekleşme ihtimali 1/ (1+ T/ t) ile formüle edilmektedir. Formülde "T" bloğun ortalama olarak bulunma süresini gösterirken "t" bulunan bloğun ortalama olarak yayınlanma süresini temsil etmektedir. Bu formül bağlamında bloğun bulunma süresinin 10 dakika yani 600 saniye olduğu ve ağda yayınlanma süresinin ortalam 10 saniye varsayımı altında örnek bir hesaplama yapılacak olursa; (1+600/10) hesaplama sonucundan 0,016 sonucu ortaya çıkmaktadır. Bu durum yaklaşık olarak günde 147 blok yaratıldığı varsayımı altında 147 bloğun %1,6'sı olarak 2,3 orphan blok olarak hesaplanmaktadır (Kurt, 2018: 69-70).

1. 6. 3. 5. Mutabakat Mekanizması (Consensus Mechanism)

Eşler arası ağda bulunan katılımcılardan herhangi biri kendilerine ait kişisel dijital hesap veri defterlerine veri girişi yapmak isteyebilirler. Bu durumda fikir birliğine varılması gerekmekte ve bu şekilde dağıtık defterler güncelenmek zorundadır. Dolayısıyla işlemler belirli algoritmalar kullanılarak kodlanmakta ve yapılan veri girişleriyle ilgili ağa kayıtlı tüm katılımcılar bilgilendirilmektedir. Burada

önemli olan nokta kullanıcılar arasında mutabakat yani uzlaşı sağlanması koşuluyla doğrulandığı takdirde veri kalıcı kayıtlara eklenmektedir. Kaydı yapılan işlemlere ise, ağa kayıtlı tüm katılımcılar aynı kayıtlı verilerle çalıştığından dolayı, itiraz edilemez ve bu işlemlere itiraz edilemediği gibi üzerinde bir mutabakata varıldığından dolayı değiştirme işlemi de yapılamamaktadır (Yavuz, 2019: 17).

Dağıtılmış ve merkezi olmayan bir ağda gerektiğinde oybirliğiyle gerçekleştirilecek işleme karar verilmesine yardımcı olan mutabakat algoritmalarının; merkezi olmayan yönetim, kimlik doğrulama, dürüstlük, reddedilmeme, hata toleransı ve performansı güvence altına alma gibi özellikleri bulunmaktadır. Mutabakatın en bilinen türü Proof of Work (PoW) ve Proof of Stake (PoS) olmakla birlikte Proof of Elapsed Time (PoET), Proof of Existence (PoE), Delegated Proof of Stake (DPoS) ve Proof of Activity (PoA) gibi farklı uzlaşı protokolleri de bulunmaktadır (Sankar, Sindhu ve Sethumadhavan, 2017: 2).

(Baliga, 2017: 5) bu bağlamda uzlaşı protokollerinin uygulanabilirliğini ve etkinliğinin belirlenmesinde etkili olan 3 temel anahtar görevi gören özellikleri aşağıdaki gibi sıralamıştır.

I. Güvenlik: Bütün düğümler aynı çıktıyı üretmektedir. Bu düğümler tarafından üretilen çıktılar protokolün kurallarına göre geçerli olursa uzlaşı protokolünün güvenli olduğu anlaşılmaktadır.

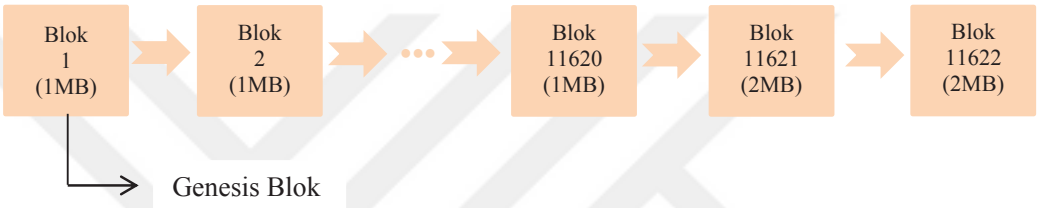
II. Canlılık: Bir uzlaşı protokolü, uzlaşıya katılan tüm hatalı olmayan düğümlerin sonunda bir değer üretirse canlılığı garanti edilmiş olmaktadır.

III. Hata Toleransı: Bir uzlaşı protokolü, uzlaşıya katılan bir düğümün başarısızlığından kurtulabiliyorsa hata toleransı sağlanmış olmaktadır.

1. 6. 3. 6. Çatallanma (Forking)

Blokzincir ağından gerçekleştirilecek işlemler bir mutabakat mekanizmasına bağlı olarak gerçekleştirilmektedir. Ancak bazı durumlarda üzerinde uzlaşıya varılmış bazı kurallarda değişiklikler veya yeni ve daha etkili olabileceği düşünülen bazı öneriler ileri sürülmektedir. Bu durumda yapılacak değişiklik önerilerinin sistem tarafından benimsenip benimsenmeme durumuna göre çatallanmalar meydana gelmektedir. Blokchain çatalları bu bağlamda soft forking (gönüllü çatallanma) ve

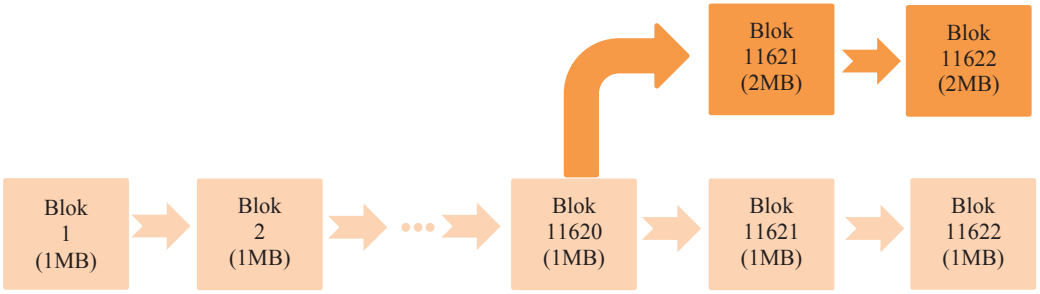
hard forking (Zorunlu- Mecburi Çatallanma) olmak üzere iki gruba ayrılmaktadır. Burada gönüllü çatallanma önceki bloklarla, geriye dönük olarak uyumlu olacak şekilde tasarlanmış evrimsel ve yinelemeli değişiklikleri temsil etmektedir. Gönüllü çatallanmanın başarısı, önerilen yeni kuralların çoğunluk tarafından benimsenmesine bağlanmaktadır (Berg ve Berg, 2017: 4-5). Gönüllü çatallanmanın 11,621 numaralı blokta uygulanmasına karar verildiği durum için gönüllü çatallanma örneği Şekil 24'de verilmiştir.



Kaynak: (Güven ve Şahinöz, 2018: 70).

Şekil 24: Gönüllü Çatallanma

Şekil 24 blok boyunun 11,621 numaralı bloğa kadar 1 MB ile sınırlandırılırken bu bloktan sonra 2 MB'ı geçmeme kuralının kabul edildiğini göstermektedir. Şekilde gösterilen gönüllü çatallaşmanın yanı sıra blokzincirde aynı zamanda mecburi çatallanma olarak adlandırılan bir başka çatallanma türünün olduğu da çalışma kapsamında yukarıda belirtilmişti. Bu bağlamda mecburi çatallanma ise gönüllü çatallanmadan farklı olarak geriye dönük olarak uyumlu olmayan blokzincir uygulamasında yapılan değişiklikler olarak ifade edilmektedir. Burada yayınlanan tüm düğümlerin güncellenmiş protokole geçmeleri ve yeni şekillendirilmiş blokları reddetmemeleri için yeni protokole yükseltilmeleri gerekmektedir. Güncellenmemiş düğümler ise, güncellenmiş blokzincirde işlem yapmaya devam edememektedir. Çünkü blok spesifikasyonunun sürümlerini takip etmeyen herhangi bir bloğu reddetmeye programlanmışlardır. Bu şekilde güncellenmemiş kullanıcı blokları yeni biçimlendirilmiş blokları reddederek sadece eski şekildeki blokları kabul etmektedir. Bu durumda aynı anda var olan blokzincir ikiye ayrılacak fakat sonraki süreçte uzlaşı yine sağlanmış olacaktır (Yaga vd., 2018:30). Bu şekilde işleyen bir blok olan mecburi çatallanmanın örneği Şekil 25'te gösterilmiştir.



Kaynak: (Güven ve Şahinöz, 2018: 70).

Şekil 25: Mecburi Çatallanma

Şekil 25'de 11.621 numaralı bloktan önceki bloklarda 1 MB blok boyutu geçerliyken bu bloktan sonra değişiklik önerilmiştir. Ancak bu değişikliği kabul eden madenciler 2 MB büyüklük kuralının her blok için aranacağını belirtirken bu yeni kural bundan önceki bloklar için geçerli olmayacaktır. Değişikliği kabul etmeyen madenciler için ise zaten bir değişiklik meydana gelmeyeceğinden dolayı aynı zincir üzerinden devam edilecektir.

1. 6. 4. Blockchain ve Akıllı Sözleşmeler

Akıllı sözleşmeler, kod ile yazılmış ve belirli bir blokzincire bağlı sözleşmelerdir. Bu kod içerisinde gerekli tüm şartlar yerine getirildikten sonra kendiliğinden otomatik olarak yürütülen tüm kural ve koşulların yanı sıra son kullanma tarihlerini ve gerçekleştirilmesi gereken tüm diğer bilgileri bulundurabilmektedir. Geleneksel ya da ilkel sözleşmelerin aksine akıllı sözleşmeler farklı bir programcı diline sahip olup önceden kurulmuş koşulları içermektedir. Bu şekilde önceden tanımlanmış şekillerde hareket etmekte ve bir koşulun gerçekleşmesi sonucunda ortaya çıkacak sonuç belirlenmekte aksi bir durum ortaya çıktığında ise gerçekleşecek alternatif bir sonuç otomatikleştirilmektedir. Yani belirli kalıplara sahiptirler ve bu kalıpların dışına çıkılamamaktadır. İlk olarak 1994 yılında Nick Szabo tarafından kavramlaştırılan akıllı sözleşmelerin ilk örneğini yiyecek ve içecek otomatı gibi dijital satış makineleri oluşturmaktadır. Burada bir öğe seçilmekte ve gerekli nakit miktarı da girildikten sonra ödeme kaydedilmekte böylelikle istenilen

ürün alınabilmektedir. Buna yazar kasa mantığı da denilmektedir. Akıllı sözleşmelerin blokzincir kullanım alanlarının genişletilmesinde öneme sahip olması ise tüm tarafların gereksinimi için tamamen nicel olan gerçekleri ortaya koymasından kaynaklanmaktadır. Yani akıllı sözleşmelerde işlemin gerçekleştirilmesi sayısal verilere dayanmaktadır (Atabaş, 2018: 69-70).

(Konukseven ve Özen, 2018: 95) bu bağlamda, akıllı sözleşmelerin avantaj sağlayan karakteristik özelliklerini 5 maddede aşağıdaki gibi sıralamıştır:

- Ekonomiklerdir. Herhangi bir işlemde bu işlemin gerçekleştirilmesi için aracılar ve komisyoncular mevcuttur. Ancak akıllı sözleşmeler bu durumu ortadan kaldırarak komisyonculara verilecek paranın cepte kamasını sağlayacaklardır.
- Otonomlardır. Akıllı sözleşmeler önceden kodlanan şartların yerine getirilmesi durumunda çalışmaktadır. Aksi durumda işlem gerçekleştirilememektedir.
- Güvenlilerdir. Akıllı sözleşmelerde kişilerin kimlikleri anonim yani gizli kalabilmektedir. Mevcut bilgiler kriptoloji aracılığıyla gizlenerek korunmaktadır.
- Yedeklilerdir. Akıllı sözleşmeler üzerinden gerçekleştirilen tüm transferler ve işlemler yedeklenmektedir.
- İsabetlilerdir. Akıllı sözleşmeler hem insandan kaynaklı hataları önlemekte hem de sürecin gerçekleşme ve oluşma süreçlerini fazlasıyla hızlandırmaktadır.

Akıllı sözleşmelerin otomatik, güvenilir ve doğrulanabilir doğası gerçekte somut blokzincir kullanımlarını ortaya çıkarmıştır. Bu bağlamda akıllı sözleşmeler, belli iş süreçlerini ifade edebilirken daha karmaşık işlemleri yerine getirebilmek için blokzincirde birleştirilebilmektedir. Akıllı sözleşmelerin bir diğer örneği ise "dapp" olarak adlandırılan blokzincir uygulamalarıdır. Dapp'lar belli bir blokzincire bağlanmak için akıllı sözleşmeleri kullanmaktadırlar. Aynı zamanda kripto paralar içerisinden "Ethereum" akıllı sözleşmelerin en yaygın platformlarını oluşturmaktadır ((Atabaş, 2018: 72-73). Bunların yanı sıra akıllı sözleşmeler ve blokzincirin bugünlerde yapılmış ve denemenin ötesine geçebilmiş birçok uygulama alanları bulunmaktadır.

(Özcan, 2019: 7-8)'de bu uygulama alanlarını ayrıntılı bir şekilde açıklanmıştır. Bunlar aşağıda verilmiştir:

I. Basic Attention Token: Javascript dilinin yaratıcısı Brendan Eich tarafından kurulmuş bir şirket olup blockchain üzerine kurulmuş merkezi yapıdan uzaklaşarak dijital reklam pazarına hitap eden ana akım kuruluşlarına karşı çıkmayı hedefleyen uygulamadır.

II. Winding Tree: Ethereum platformu üzerinde çalışmakta olan bir akıllı sözleşme uygulaması örneğidir. Havayolu taşımacılığı ya da biletleme gibi alanlarda işlemlerin hızlandırılmasını hedeflemektedir.

III. Bob's Repair: Hizmet alışverişi yapanlar arasında bağlantıyı kurabilmek amacıyla kurulan bir blokzincir uygulamasıdır.

IV. SilentNotary: Zamandan tasarruf sağlayarak hızlı değiş tokuş işlemi yapılmasına olanak sağlayarak noterlik sistemini akıllı sözleşmeler üzerinden gerçekleştirmektedir.

V. Poet: Blockchain üzerinde güvenilir ve şeffaf yapı oluşturarak sanat eserlerinin lisanslanmasına olanak sağlayan bir uygulamadır.

VI. Storjcoin: Merkezi olmayan ve bokzincirin gücünü ortaya koyan bir depolama sistemidir.

VII. PowerLedger: Üretilen elektriği dolaşıma girdirip karşılığında blockchain üzerinden para kazanılmasına olanak sağlamaktadır.

VIII. Te-food: Asya merkezli bir şirket olarak hayvanların kesilmesi ve beslenmesi gibi birçok aşamayı blokchain üzerinden kullanıcıya sunmaktadır.

IX. Vinchain: Merkezi olmayan taşıt kaydı oluşturmayı hedeflemektedir.

İKİNCİ BÖLÜM

KRİPTO PARA EKONOMİSİ: BİR BLOCKCHAİN UYGULAMA ALANI OLARAK BİTCOİN VE ALTCOİNLER

Çalışmanın bu bölümünde öncelikli olarak kripto paraların üretilmesinde ve işlemesinde önemli payı olan madenciler ve madencilik kavramı açıklandıktan sonra kripto para cüzdanlarına değinilmiştir. Ayrıca temel kripto para birimi olan Bitcoin ayrıntılı bir şekilde açıklandıktan sonra Altcoinler ile ilgili bilgi verilmiştir. Böylelikle kripto para türleriyle ilgili literatürdeki bilgi yetersizliği azaltılmıştır. En son ise kripto para ekonomisi açıklanmıştır. Bu başlık altında ülkelerin kripto paralara yaklaşımları, kripto paraların vergilendirilmesi ve kripto paralarda arbitraj uygulamasına değinildikten sonra Türkiye'de ve dünya'da işlem gören kripto para borsaları açıklanmıştır.

2. 1. KRİPTO PARA MADENCİLİĞİ (MİNİNG)

Blokzincir sistemi üzerinden kripto para çıkartma ya da para basma işlemine madencilik denilmektedir. Madencilik sisteminde ise işlemler bilgisayar sistemi üzerinden, bilgisayarların gücü doğrultusunda matematiksel algoritmaları çözerek yapılmaktadır. Madencilik işlemlerini yapan kişilere ya da bilgisayarlara da madenciler denilmektedir. Kripto para madencileri denilen bu kişiler veya bilgisayarlar ise alışveriş yapılırken bilgileri doğrulamakta, mevcut bilgilerin güncellenmesini yaparak güvenilir bir alışveriş yapılmasına yardımcı olmaktadırlar. Yani kripto paraları kapsayan hesap defterlerinde hata olmamasını sağlamakla ilgilenmektedirler. Burada önemli olan nokta bu defterlerin tüm bilgisayarlarda eşanlı olarak aynı şekilde bulunmasıdır. Bu gerçekleştirilen bir transfer işleminin ardından kişilerin gerçekleştirilen işlemlere itiraz etme hakkının bulunmadığı anlamına gelmektedir (Abaday,2018: 39).

Madencilik bu bağlamda kripto para işlemlerinin doğrulama süreci olarak da ifade edilebilmektedir. Bu süreç ayrıntılı bir şekilde açıklanacak olursa ağdaki katılımcılar blok olarak adlandırılan ve giderek zorlaşan matematiksel denklemleri her 10 dakikada bir çözmektedirler. Her bloktaki bir işlem bir önceki bloğa bağlı olarak işlenmektedir. Dolayısıyla herhangi bir bilginin değişmesi birçok bilginin değiştirilmesini zorunlu kılmaktadır. Bu işlemin kolay olmaması ise değiştirme işlemini neredeyse imkânsız hale getirmektedir. Dolayısıyla bu kadar zor bir şekilde işleyen bir sistem içerisinde madencilerin; bilgilerin doğrulanması, güncellenmesi ve güvenliğini sağlayarak yeni bir blok çözmesi gibi görevleri bulunmaktadır. Bu işlemleri gerçekleştiren madenciler ise ödüllendirilmektedir. Yani madenciler bir bloğu doğru şekilde çözdükleri herhangi bir zamanda işlem ücretleri almakta ve küçük bir ödüllendirmeye tabii tutulmaktadırlar. Örneğin 21 milyon sınırına ulaşana kadar, yarattıkları her yeni Bitcoinler karşılığında küçük bir miktar Bitcoin ile ödüllendirilmektedirler. Bu ödüllendirmeler ise yeni kripto paraların piyasaya arz edilmesine olanak sağlamaktadır. (Demartino, 2016/2018: 222).

Madencilerin ödüllendirilmesi durumu Bitcoin özelinden değerlendirilecek olursa Bitcoin'de ödül ilk başlarda 50 BTC iken her 210,000 blokta bir ödül yarıya düşmektedir. Her 10 dakikada, bir blok kaydı yapıldığı ve 2012 Kasım ayında ödülün 25 BTC'ye düştüğü bilgisinden hareketle de bu BTC ödülünün son zamanlarda giderek daha da düşmesi beklenmektedir (Çeker, 2018: 13-14). Tüm bu durumlar kripto para işlemlerinde madenciliğin olmazsa olmaz bir kavram haline geldiğini göstermektedir. Dolayısıyla çalışmanın bu başlığı altında kripto paralar için bu kadar önemli bir yere sahip olan madencilik işlemleri ve madencilik kavramı ayrıntılı bir şekilde açıklanmıştır.

2. 1. 1. Kripto Para Madencileri Ne İş Yapmaktadır?

Kripto para madenciliği resmi olarak blokzincir adıyla bilinen ve halka açık bir muhasebe defteri üzerinden işlemleri onaylama ve ekleme süreci olarak tanımlanmaktadır. Dolayısıyla madencilerin temel olarak görevi bir takım matematik problemleri bilgisayar kullanarak çözmek ve ağdaki işlemlerin veya bloğun geçerliliğini doğrulamaktır. Diğer yandan madencilerin yaptığı işlemler aşamalar halinde; eklenmiş olan işlemlere bakmak, bu işlemleri onaylamak, işlemleri blokların

içine paketlemek ve son olarak SHA-256 + (veri) + (bir kerelik rakam) gibi bir numarayı tahmin etmek olarak sıralanmaktadır. Burada son adım olan SHA-256 bir şifreleme algoritması olup çalışmanın birinci bölümünde ayrıntılı bir şekilde açıklanmıştır. Bir kerelik rakam denilen kavram ise madenciler tarafından tahmin edilen rastgele bir tamsayıyı ifade etmektedir. Veri de blok içerisindeki özeti ve önceki bloğun özetini belirtmektedir. Bu işlemde zorluk derecesi, hedefe ulaşmak için hash'i çözmenin zorluğundandır. Bu zorluklar ise sadece belirli kişilerin mi madencilik işlemini yapabileceği sorularını gündeme getirmektedir. Bu noktada elinde uygun donanımı ve interneti olan herkesin madenci olabileceğinin belirtilmesi gerekmektedir. Burada önemli olan nokta madencilik için iyi bir donanım, iyi bir madencilik yazılımı ve bir kripto para cüzdanına sahip olunmasıdır. Bu özellikleri elinde bulunduran kişiler madenci olabilmektedir (Nebil, 2018: 56-57).

2. 1. 2. Madencilik Çeşitleri

İlk zamanlarda normal bilgisayar ekranları aracılığıyla işlemler gerçekleştirilebilirken zaman içerisinde, blok sayılarının artmasına bağlı olarak, işlemlerin gerçekleştirilebilmesi için yeni ekran kartlarına, yeni programlara ve işlemcilere ihtiyaç duyulmuştur. Bu durum da madenciliğin farklı şekillerinin ortaya çıkmasına neden olmuştur. Çalışmanın bu bölümünde madencilik çeşitlerinden ekran kartı ile madencilik, bulut madenciliği ve madencilik havuzlarından bahsedilmiştir (Durmuş ve Polat, 2018: 665).

2. 1. 2. 1. Ekran Kartı ile Madencilik

Madenciliğin ilk zamanlarında oyuncu kartları ile madencilik yapmak oldukça kolaylaşmış ve global piyasada ekran kartı bulunmaz hale gelmiştir. Bu kartların, haftanın her günü ve her saatinde tam performanslı olarak çalışacak şekilde tasarlanmamasından dolayı da birkaç ay gibi kısa bir süre içerisinde performans düşüklüğü kendini göstermeye başlamıştır. Bu durum sadece madenciliğe yönelik ekran kartı üretilmesi fikrini ortaya çıkarmış ve madencilik için olan ekran kartları piyasaya sürülmüştür. Bu sayede oyuncu kartlarından daha uygun ücretlerle, sadece madenciliğe yönelik olan ekran kartlarının alınmasına imkân sağlanmıştır (İnci ve Alper, 2018: 57).

Dünyanın birçok yerinde, her geçen gün sisteme katılan yeni işlemcilerin sayısı biraz daha artarak işlem gücünün devasa boyutlara ulaşmasına neden olmuştur. Bu bağlamda getirisindeki avantajlardan dolayı ekran kartı teknolojisine dayalı GPU madenciliği giderek daha çok yaygınlık kazanmıştır. Ancak son zamanlarda Bitcoin zorluk seviyesindeki yükselmelerin etkisiyle, ekran kartı ile madenciliğin gelir gider dengesinde kârlı bir işlem olmadığı anlaşılarak tercih edilmez olmuş ve madencilere özel üretilen işlemciler, GPU madenciliğinin yerini almıştır. Bu bağlamda ASIC'ler madencilik için kâr elde edilebilecek bir zorluk seviyesine ulaşmış ve GPU'ların yerini almayı başarmıştır. Ancak bu durum GPU madenciliğinin tamamen ortadan kalktığı anlamına gelmemektedir. Başta Ethereum olmak üzere Altcoin çıkartan ve alım-satım yapan kişiler için ekran kartı madenciliği hâlâ önemli bir yere sahiptir (Yıldırım, 2015: 89).

2. 1. 2. 2. Bulut Madenciliği

Madencilik maliyetlerinin zaman içerisinde giderek artmasıyla birlikte madenciliğin bireysel olarak yapılması neredeyse imkânsız hale gelmiş ve bu durum "Bulut Madenciliği" olarak adlandırılan bir kavramın ortaya çıkmasına neden olmuştur. Bulut Madenciliği, bir şirket tarafından gerekli madencilik donanımlarının kiralaması anlamına gelmektedir. Bu kiralama işlemi; sabit ve belirli bir fiyattan, bir süreliğine ya da ömür boyu kullanıcılar için madencilik yapılmasına olanak sağlamaktadır. Ancak avantajlı bir yapı gibi görünmesinin yanında kontrol eksikliği, kiralama yapılan şirketin güvenliği, ödenmesi gereken ücret miktarları ya da şirketlerin savunmasız olmaları gibi bazı dezavantajlarının bulunduğunun da belirtilmesi gerekmektedir. Yani bulut madenciliği yapmayı isteyen kişilerin dolandırılma riski olduğunu da bilerek yapmaları gerekmektedir (Güleç, Çevik ve Bahadır, 2018: 25).

Bulut madenciliği yöntemi ile madencilik havuzlarına dâhil olmakta mümkündür. Ancak bu noktada bulut madenciliği ile madenci havuzlarının birbirleriyle karıştırılmaması gerekmektedir. Çünkü madenci havuzlarında madencilik için kullanılan cihazlar elde mevcut bulunurken, bulut madenciliğinde elde cihazın olup olmamasıyla ilgilenilmemekte sadece belirli ve küçük miktarlarda bir ücret ve bir gelir talep edilmektedir (İnci ve Alper, 2018: 57-58). Talep edilen bu

kiralama ücretleri farklı kripto paralar için değişiklik göstermekle birlikte kiralama ücretlerinin genel olarak bir kazma işlemi başına 1.30-1.40 USD olarak değiştiği bilinmektedir. Ancak kripto paraların öncüsü olan Bitcoin için kiralama ücreti 0.80 USD olup diğer kripto paralardan daha düşüktür. Buradan diğer kripto paraların madenciliğinin Bitcoin madenciliğine göre daha çok kazanç getirdiği sonucu çıkarılabilmektedir (Çeker, 2018: 15).

2. 1. 2. 3. Madencilik Havuzları

Mining Pool olarak adlandırılan madencilik havuzları, madencilerin bir blok bulma ihtimalini artırmak için kaynaklarını yani madencilik güçlerini bir araya getirme yolu olarak tanımlanmaktadır. Bu havuzlar, madencilik yazılımını ve komut dosyalarını sürdürme görevinin bulunmasıyla birlikte asıl görevi her bir madencinin hash oranını ve üretilen bloklara katkısını tahmin etmektir. Bu amaçla madencilik havuzu operatörü her madenci için bir PoW problemi göndermektedir. Bu noktada madenciler, havuzun problemini çözmede sürekli olarak hesaplama gücü kullanarak havuza katılmaktadırlar. Bir madenci her çözüm bulduğunda, madencilik havuzunun yanında bulunan blok için bir pay sunulmaktadır. Bazen madencilik havuzunun sorununa gönderilen çözüm, daha zor ağ sorununa da bir çözüm olabilmektedir (Zamyatin vd., 2017: 101).

Madencilerin çoğu, hesaplama çabalarının verimliliğini en yüksek düzeye çıkarmak için madencilik havuzlarını kullanmaktadırlar. Bir pool ise bir web sunucunda ya da özel bir sunucuda bulunan bir yazılımdır. Burada madenciler, havuz sunucusunda hesaplar oluşturmakta ve daha sonra madencilik yazılımlarının yapılandırma dosyalarına havuz kimlik doğrulama bilgilerini eklemektedirler. Kimlik doğrulandıktan sonra ise daha verimli bir donanım kullanımını sağlayacak dağıtılmış bir işlem ağındaki kaynakları paylaşmaktadırlar. Sonuç olarak bu işlemlerin sonucunda madencilik havuzu bir sonraki bloğu üretecek ve madencide kripto para birimi ağından blok ödülünü alacaktır. Ancak burada önemli olan nokta havuzda madencinin katkısına ve ödül ödeme planına göre havuzun madencileri arasında dağıtılacaktır. Yani havuzlarda bloğu bulan cihaz, sadece havuz sistemi tarafından bilindiğinden dolayı herhangi bir şekilde bir kullanıcının ödülün tamamını isteme hakkı bulunmamaktadır (Heid, 2013).

2. 1. 3. Madencilik Onay İşlemi

Çalışmanın birinci bölümünde katılımcıların gerçekleştirilen bir işlemi kabul edip etmeme hakkının olduğu söylenerek yeterli sayıda madencinin bir konuda onaylama işlemi yapmak için uzlaşıya varması gerektiği ve ancak bu şekilde işlemlerin onaylanabileceği belirtilmiştir. (Bkz: 1. 6. 3. 5.). Çalışmanın bu bölümde de en yaygın uzlaşı protokolü olarak bilinen ve madencilerin onaylama işlemini gerçekleştirdiği Emek ispatı (Proof of Work - PoW) ve Pay kanıtı (Proof of Stake - PoS) ayrıntılı bir şekilde açıklanmıştır.

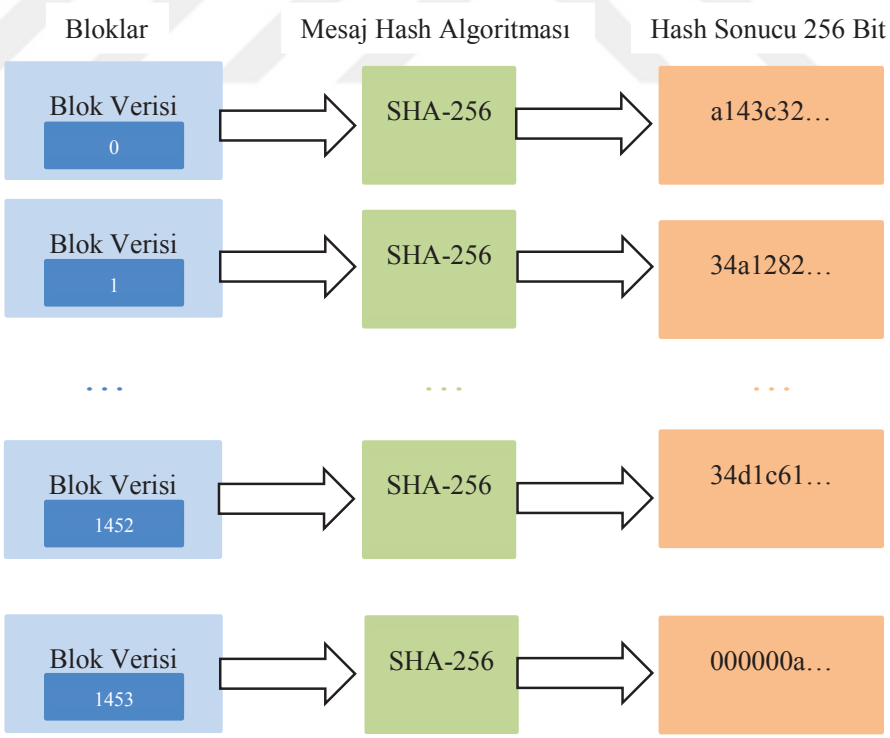
2. 1. 3. 1. Emek İspati (PoW)

Emek Kanıtı terimi ilk olarak 1992 yılında Cynthia Dwork ve Moni Naor tarafından istenmeyen e-mail'ler ile mücadele etmek amacıyla kullanılmıştır. PoW hizmet saldırılarını önlemek için ekonomik bir yöntem olarak ifade edilmektedir. Burada istekte bulunan servis ya da kişilerden bazı hesaplama işlemlerinin yapılması istenmektedir. Bu yöntemin en önemli özelliği asimetrik olması olup kullanıcıların sisteme erişebilecekleri bir fonksiyonu hesaplamak için işlem gücünü kullanmaları gerekmektedir. Bu hesaplama, istekte bulunan taraf için orta derece zorluğa sahiptir. Ancak bu hesaplamanın mümkün olmadığı anlamına gelmemektedir. Yani kaynağa ulaşarak gereksiz kullanımları önlemek için kullanıcıların orta dereceli ve zorlu olmayan bir işlevi hesaplamaları gerekmektedir. Servis sağlayıcının işlemi kontrol emesi ise oldukça kolay olmaktadır (Kardaş, 2019: 485).

1992 yılından yaklaşık 5 yıl sonra ise Dwork ve Naor tarafından sunulana benzer bir işlevi Adam Back hashcash ismi ile duyurmuştur. Hashcash, e-postaların spam olup olmadığının anlaşılması için SHA-1 şifreleme algoritmasını kullanmıştır. Satoshi Nakamoto'da bu hashcash yönteminden esinlenerek Bitcoin dağıtılmış defterlerde kullanılan madencilik işlevi için ilham kaynağı olmuştur. Bu doğrultuda Back'in Dwort ve Naor'dan; Nakamoto'nun da Back'ten esinlenerek oluşturduğu Bitcoin mutabakat yapısı SHA-256 şifreleme algoritmasının iki defa uygulanması yöntemini esas almaktadır. Yani aslında bu yöntemde iki kat işlem yapılmaktadır. Bu doğrultuda Bitcoin ortamında saniyede quintillion'larca hash işlemi yapıldığı bilinmekte ve ortalama 10 dakikada bir blok üretilmektedir. Bloktaki veriler kullanılarak, çalışmanın önceki bölümünde de belirtildiği üzere, merkle ağacı ve

merkle kök değeri, bir önceki bloğa ait özet değeri, zaman bilgisi ve son olarak nonce değeri kullanılarak blok başlığı oluşturulmaktadır. Daha sonra blok başlığının SHA-256 algoritma fonksiyonundan iki defa geçirilmesinin ardından uygun bir değer oluşup oluşmadığı kontrol edilmektedir. Bu uygunluk gerçekleştiği takdirde bilgi ağdaki tüm düğümler ile paylaşılmaktadır. Ancak uygunluğun sağlanmadığı durumda nonce değeri sınırına ulaşana kadar artırılarak işlem tekrar denenmektedir. Bu şekilde 2 kat işlem yapılarak gerçekleştirilen emek ispatı, blockchain platformunda en yaygın olarak Bitcoin'lerde kullanılmaktadır. Ancak PoW yönteminde de yüksek enerji, özel donanıma ihtiyaç duyulması ve artan blok boyutuna bağlı olarak blok üretim süresinin atması gibi dezavantajlar da bulunmaktadır (Aldemir, 2018: 28-29).

Emek ispatı yönteminde bulmacayı çözme ile yeni eklenecek bloğu bulma işlemi Şekil 26'te gösterilerek emek ispatının işleyiş süreci gösterilmiştir.



Kaynak: (Taş ve Kiani, 2018: 373).

Şekil 26: PoW Protokolünde Bulmaca Çözme ile Yeni Eklenecek Bloğu Çözme

2. 1. 3. 2. Pay Kanıtı (PoS)

PoS yöntemi ağdaki işlemleri doğrulayarak onaylamanın bir diğer yoludur. Bu metodun özelliği kullanıcıların yeni bir para üretmeleri için işlem yapmalarına gerek bulunmamasıdır. Bundan dolayı da bu yöntem aslında madencilik olarak değil para basma olarak değerlendirilmektedir. Bu yöntemde, cüzdanda bulunan para miktarıyla orantılı olarak ödül kazanılacağından dolayı, para kazanmak isteyen kullanıcıların mevcut elektronik cüzdanlarında para bulundurmaları gerekmektedir. Bu elektronik cüzdanda ne kadar çok para bulunursa o kadar çok ödül kazanılacak ve para üretilebileceği anlamına gelmektedir (Mendi ve Çabuk, 2018: 16).

PoW yönteminde gücün artırılabilmesi için madencilik yapılan cihazların sayısının veya gücünün artırılması gerekirken PoS yönteminde cüzdanda sahip olunan kripto para oranının artırılması gerekmektedir. PoS yönteminde sonraki bloğu üretecek olan makinenin öncelikli olarak sistem içerisindeki payına bakılmakta ve payı en yüksek olan hangisi ise o seçilmektedir. Bu durumda seçilen makinenin, uygun bir süre içerisinde blok üretme işleminin gerçekleştirememe ihtimali bulunmaktadır. Böyle bir durumda sonraki makineye geçilmektedir. Burada en yüksek paya sahip olan makinelerin sürekli olarak ilk üretim önceliğine sahip olmalarını düzenlemek amacıyla ise yaş kavramı geliştirilmiştir. Böylelikle blok üretiminde kullanılmakta olan pay kapsamındaki paraların yaş değerleri sıfırlanmakta ve bu kripto paralar bir süre sonra yaş almaya başlamaktadır. Bu kapsam da para üretimi denilen kavram, bu blok üretim sürecine denilmektedir. Bu işleyiş altında PoS yönteminin avantajı; işlemlerin doğrulanması, blok üretim sürecini hızlı ve daha kolay bir hale getirmesi, PoW yönteminin pahalı ve yüksek enerji tüketim problemlerini ortadan kaldırmasıdır. Bu avantajlara bağlı olarak da kripto paralar içerisinde Bitcoin'den sonra en yaygın olan ve özellikle son zamanlarda popülerliği giderek artan Ethereum da PoW yönteminden PoS yöntemine geçme hazırlığı yapmaktadır. Benzer şekilde mevcut kripto para birimlerinin bazıları PoS yöntemine geçmekte ve yeni çıkan kripto paralarda PoS yöntemini seçmektedir (Aldemir, 2018: 30).

2. 1. 4. Madencilik Ücretleri (Mining Fees)

Kripto para birimlerinin bir kişiden bir diğer kişiye transferi blockchain sistemi üzerinden gerçekleşmekte ve bloklardan oluşan bu sistem üzerine

kaydedilmektedir. Kripro para madenciliği yapmak isteyen kişiler ve kuruluşlar bu bloklar üzerinden işlemlerini gerçekleştirmektedirler. Bu bağlamda madencilerin temel görevi belirli yazılım programları ve yüksek işlem gücüne sahip donanımlar vasıtasıyla yeni bloklar bulmaya çalışmaktır. Madenciler, buldukları her bloklar karşılığında ise belirli bir ücret almaktadırlar. Bitcoin örneklemi üzerinden incelenecek olursa, sistem arz fazlalığını engelleyebilmek amacıyla her 210,000 blok tamamlandıktan sonra madencilerin kazanacağı ücret seviyesini yarıya düşürmektedir. Bitcoin'in Nakamoto'nun makalesiyle gündeme geldiği 2008 yılında madenciler tarafından bulunan bloktan her madenci 50 BTC kazanırken her blok için şu anda 12,5 BTC kazanmaktadırlar. Bu kazanılan ücret ya da ödül ise her 4 yılda bir yarılanmaktadır. Bu şekilde blok bulmanın zorluk seviyesi giderek daha da artmakta ve arz miktarının belli bir hızda sürekli olarak azalarak artması sağlanmaktadır. Bu şekilde işlemesinin altında ise Bitcoin'in toplam arz miktarının 21 Milyon adet olacak şekilde tasarlanmasından kaynaklanmaktadır (Özbaş, 2019: 93-94).

2. 1. 5. Madencilik Cihazları

Madencilik faaliyetleri ilk başlarda işlemci tabanlı olup işlem gücüyle hesaplama yaparak kripto para üretebilirken daha sonraları ekran kartlarının kullanıldığı cihazlar kullanılarak kripto para madencilik işlemi gerçekleştirilmiştir. Ancak zaman içerisinde özellikle Bitcoin madenciliğine olan ilginin sürekli artmasına bağlı olarak bu işlem gücü ve ekran kartı kullanılan cihazlar, madencilik faaliyetlerinin verimliliğini azaltarak yetersiz kalmıştır. Buna bağlı olarak Bitcoin madenciliği uygulamaya özgü tümleşik devrelerin kullanıldığı ASIC cihazları çıkarılmış ve bu cihaz sayesinde fayda sağlanabilecek zorluk seviyesine ulaşılmıştır. Çalışmanın bu bölümde ise madencilik işleminin gerçekleştirilmesi için büyük bir öneme sahip bu cihazlar kısaca açıklanmıştır (Boran Güneysu ve Memiş, 2018: 84).

2. 1. 5. 1. GPU Ethereum Madencilik cihazı ve RİG

Ethereum çıkarabilmek için grafik işleme birimi yani GPU olarak bilinen özel bir donanıma gereksinim duyulmaktadır. Ethereum ilk başlarda ortalama bir bilgisayar işlemcilerinin çalışması aracılığıyla çıkarılabilecek şekilde çalışmasına karşın zaman içerisinde gelişmiş GPU'lar ile çalışılmaya başlanmıştır. Bu bağlamda

GPU, özel bir Ethereum madencilik bilgisayarı olarak nitelendirilmektedir. Sistemde Ethereum Directed Acyclic Graph (DAG) dosyası, madenciler tarafından VRAM'de saklanmaktadır. Madencilik zorlaştıkça DAG'da oranda büyümektedir. Ethereum madenciliği günümüzde en az 3 GB'lık video RAM yani VRAM içeren bir GPU gerektirmektedir. Ethereum madencilik donanım üreticileri ise AMD ve Nvidia'dır. İlk dönemlerde AMD, Nividia'nın önüne geçmiş ancak daha sonraları Nvidia'nın Titan serisi kartları AMD ile aralarındaki farkı iyice azaltmıştır. İkisi arasındaki fark net bir şekilde belirtilecek olursa da AMD kartları daha ucuz olmakla birlikte Nvidia, Microsoft Windows ile daha iyi çalışmaktadır. Bu noktada çalışma kapsamında GPU'nun sadece Ethereum ile açıklanması, GPU madencilik cihazlarının sadece Ethereum'da mı kullanıldığı sorusunu akla getirmektedir. Bu noktada Ethereum'un dışında Monero, Zcash, Vertcoin ve Ethereal Classic gibi yaklaşık 40 farklı Altcoin'in madenciliğinde de GPU'dan yararlandığının ayrıca belirtilmesi gerekmektedir (Nebil, 2018: 65-66).

2. 1. 5. 2. ASIC Bitcoin Madencilik cihazı

Bitcoin'in ilk çıktığı zamanlarda madenciler bilgisayarların işlem gücüyle hesaplama yapabilmekteydiler. O zamanlarda Bitcoin üretimi için normal bilgisayarların işlem gücü yeterliyken zorluk derecesinin giderek artmasına bağlı olarak bu bilgisayarlar hem işlemin yerine getirilmesinde hem de elektrik maliyeti gibi bazı maliyetlerin karşılamasında yetersiz kalmıştır. Buna bağlı olarak ASIC-Application Specific Integrated Circuit (Uygulamaya Özel Tümleşik Devre) cihazları Bitcoin için geliştirilmiştir. ASIC teknolojisinin spesifik doğası gereği yalnızca Bitcoin madenciliği yapabilen özel ASIC'lar bulunmaktadır. Bu ASIC cihazları sayesinde ise GPU madenciliğindeki donanım ve elektrik masrafı gibi dezavantajlar ortadan kaldırılmış ve ASIC cihazının daha fazla işlem gücüne sahip olduğu anlaşılmıştır. Buna bağlı olarak da ASIC madenciliğinin Bitcoin madencileri arasındaki popülerliği giderek artarken GPU'lar daha geri planda kalmıştır (Ahamad, Nair ve Varghese, 2013: 47).

ASIC cihazlarının ne kadar büyük bir güce sahip olduğunu açıklamaya yönelik bir örnek verilecek olursa; 4 GPU çalıştırılarak kazı yapan bir donanım 3.4 MH/s gibi bir hash oranı yakalayarak 3600 kW/h tüketirken, ASIC cihazı 6 TH/s

kazarak 2200 kW/h tüketmektedir. Ardaki bu fark ASIC cihazlarının GPU ile kazma metodunu nasıl geride bıraktığının anlaşılmasını kolaylaştırmaktadır. (Azman, 2018: 68). Ancak madencilik yapabilmek için ASIC cihazının tek bir bilgisayarda bulunmasının yeterli olmayacağının belirtilmesi gerekmektedir. Çünkü "solo mining" olarak da bilinen tekli madencilikle problemi çözmek artık neredeyse imkânsız hale gelmiştir. Bu imkânsızlığın sonucunda ise çoklu kullanıcıların oluşturduğu ve "mining pool" olarak bilinen madencilik havuzlarında kullanıcılar tek bir bilgisayar yerine yüzlerce hatta binlerce madencinin katılımıyla birlikte çok daha fazla işlem gücüyle üretim yapmaktadırlar (Kurt, 2018: 63). Madencilik Havuzları çalışmanın önceki bölümünde ayrıntılı bir şekilde açıklanmıştır. (Bkz: 2.1.2.3.)

2. 2. KRİPTO PARA CÜZDANLARI: ELEKTRONİK CÜZDAN

Blokzincir üzerinden kripto paraları transfer edebilmek için kişilerin kendilerine ait dijital imzalarının bulunması gerekmektedir. Dolayısıyla kripto paralara erişip bunları kullanabilmek için kripto para sahiplerinin, dijital imzaları oluştururken aynı zamanda kullandıkları anahtarları da yönetmeleri gerekmektedir. Çünkü internet üzerinden gerçekleştirilen sanal para işlemlerinde alışverişin güvenli bir şekilde gerçekleşebilmesi için asimetrik şifreleme yöntemleri kullanılmaktadır. Anahtar yönetimi ise bilişim güvenliği alanında ayrıca üzerinde durulup dikkat edilmesi gereken bir konunun temelini oluşturmaktadır. Çünkü anahtarların başka kişiler tarafından ele geçirilmesi bazı önemli riskler içermektedir. Kripto para dünyasında ise bu şifreleme anahtarlarının başka kişiler tarafından ele geçirilmesi finansal kayıplarla sonuçlanabilmektedir. Anahtar yönetimiyle ilgili bir diğer önemli konu ise kişinin istediği kadar farklı anahtarlar yaratarak, istenildiği kadar dijital kimlik ile alışveriş yapılabilmesidir. Birden fazla dijital kimliğin ve anahtarların ise etkin bir şekilde yönetilmesi ayrı bir önem teşkil etmektedir. Bu noktada kripto para cüzdanları denilen yazılımlar aracılığıyla bu etkinlik sağlanabilmektedir (Ünsal ve Kocaoğlu, 2018: 57).

Verilen cüzdanların dışında birçok kripto para cüzdanının olduğu ve bunların sadece bir örnek olarak verildiği belirtilerek kripto para cüzdanlarına ait belli başlı yazılım örnekleri Tablo 8'de verilmiştir.

Tablo 8: Kripto Para Cüzdanları

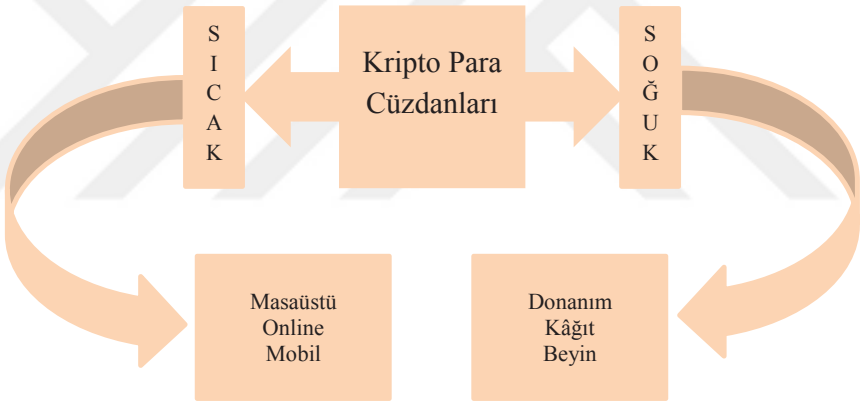
Site	Geçerli Olduğu Ülke	Ödeme Tarzı	Komisyon	Sigorta Durumu
COINBASE	25 Farklı Ülke	Banka Havalesi KK / Banka Kartı	Dönüşüm Komisyonu	Var
COINHOUSE	Avrupa (SEPA)	Kredi Kart, Neosurf, Bank Transferi	%6 - %10	-
PAXFUL	Global	P2P	%1	-
BUY A BITCOIN	Avustralya	Cash Deposit	0.0001 BTC	-
LIBERTYX	USA	Cash	%1 - %8	-
GEMINI	USA, Kanada, UK	Bank Wire	Dinamik	FDIC
LOCAL BITCOINS	Global	P2P	%1	-
WALL OF COINS	Global	P2P	%1- %2	-
ANX PRO	Hong Kong	Banka Havalesi	Var	-
CANADIAN BITCOINS	Kanada	Nakit/ XpressPost	Var	-
BitQuick	USA	Nakit Deposit	%2	-

Kaynak: (Nebil, 2018: 203).

Elektronik cüzdanlar aracılığıyla kullanıcılar kripto paralarını almakta, saklamakta ya da trasfer edebilmektedirler. Yani herhangi bir alışveriş yapmak isteyen kişiler kripto parayı kendi sanal cüzdanından, ödeme aracı olarak kabul eden karşı tarafın sanal cüzdanına göndermekte ve bu şekilde alışveriş işlemini gerçekleştirerek istediği bir mal ya da hizmete ulaşabilmektedir. Ancak diğer tüm işlemlerde olduğu gibi bu noktada da kripto para gönderme işlemi madenciler tarafından onaylanarak blokzincire eklenmekte ve tüm kullanıcıların bilgisayarına eklenmektedir. Aynı zamanda kripto para cüzdanları için kullanıcıların kişisel bilgilerini kullanmasına gerekte bulunmamaktadır. Bu şekilde de kripto araların temel prensibini oluşturan güvenlik unsurunun sağlanmasında bu cüzdanlar büyük bir öneme sahip olmaktadır (Kaplanhan, 2018: 109).

Elektronik cüzdanlar bu bağlamda en genel tanımıyla, kullanıcıların kendisine ait kripto paralarla işlem yapabilmesi için gerekli olan kişisel anahtarların saklanmasına olanak sağlayan yazılım ya da uygulanmalar olarak tanımlanmaktadır. Elektronik cüzdanlar birçok şekilde kendini göstermektedir. Bu noktada dikkat edilmesi gereken kritik nokta, cüzdanda saklanan paranın kendisi değil, işlemlerin

geçerli olacak şekilde onaylanmasına imkan veren ve kamuya açık kripto para adreslerine ulaşmayı sağlayan datanın olmasıdır (Gültekin ve Bulut, 2018: 87). Kripto para cüzdanları temel olarak ise sıcak ve soğuk para cüzdanları olmak üzere iki farklı şekilde kendini göstermektedir. İki cüzdan arasındaki temel fark ise internete bağlı olup olmamasıyla ilgilidir. Bu noktada soğuk cüzdanlar, bilgilerin çalınma riskini en aza indirmek ve saldırı riskini azalmak için çevrimiçi olmayan bir cüzdan adresinde tutulmaktadır. Sıcak cüzdanlar ise soğuk cüzdanlardan farklı olarak çevrimiçi olarak erişilebilen cüzdanlar olup bunların güvenliğinden çevrimiçi cüzdan hizmeti veren firmalar sorumludur. Bu cüzdan türleri Şekil 27'de özet halinde gösterilmiştir. (Bakan ve Şekkeli, 2019: 2852).



Kaynak: Yazar Tarafından Oluşturulmuştur.

Şekil 27: Kripto Para Cüzdanları

2. 2. 1. Sıcak Cüzdanlar

İnternete bağlı olan bu sıcak cüzdan kendi içerisinde masaüstü, online ve mobil cüzdanlar olmak üzere üç farklı türe ayrılmaktadır. Bunlar sırasıyla ayrıntılı bir şekilde açıklanmıştır.

I. Masaüstü Cüzdanlar: Masaüstü cüzdanların en önemli özelliği kullanıcının işletim sistemi üzerinden çalışan bir uygulama olmasıdır. Yani

kullanıcının bilgisayarına indirebileceği bir cüzdan türüdür. Dolayısıyla da indirilerek kurulmakta olup sadece indirilen bilgisayarda bulunmaktadır. Masaüstü cüzdanlar doğrudan Bitcoin ağına bağlıdırlar. Bu özelliğe bağlı olarak, Bitcoin üzerinde kontrol sahibi olmak isteyen kullanıcılar için masaüstü cüzdanlar uygun bir cüzdan türü olabilmektedir. Ancak herhangi bir virüs ya da hacklenme durumu gibi risklere bağlı olarak çalıştığı işletim sisteminde ya da donanımda bazı sorunlarla karşılaşılabilmekte ve cüzdana tekrar ulaşımakta bazı zorluklar yaşanabilmektedir. Bu durumda eğer yedekleme yapılmadıysa cüzdanda bulunan bütün paralar kaybedilebilmekte ve bunlara tekrar ulaşılması mümkün olmayabilmektedir (Alnıaçık, 2019: 25).

II. Online (Çevrimiçi) Cüzdanlar: Genelde bulut üzerinde çalışmakta ve internete bağlanan her cihazda kullanılabilmektedir. Erişim masaüstü cüzdanlara karşı daha kolaydır ancak bu kolaylığa karşın özel anahtar kişinin kendisinde değil görevli olduğunu iddia eden kişiler ya da hizmet sağlayıcılar tarafından kontrol edilmektedir. Kısacası saldırı ve hırsızlıklara karşı açık bir cüzdan türüdür (Abaday, 2018: 70).

III. Mobil Cüzdanlar: Mobil cüzdanlar kriptolu yani şifreli bir cüzdan türüdür. Cep telefonunda bulunan bir uygulama olup mobil alışverişlerde kolaylık sağlamaktadır. Ancak telefonun çalınma, kaybolma ya da bozulma risklerine karşın güvensiz bir cüzdan türüdür. Bundan dolayı da çok fazla tercih edilen bir cüzdan türü değildir (İşler, Takaoğlu ve Küçükali, 2019: 75).

2. 2. 2. Soğuk Cüzdanlar

Soğuk cüzdanlar internete bağlı olmayan cüzdanlar olup sıcak cüzdanlarda olduğu gibi kendi içerisinde 3 farklı türe ayrılmaktadır. Bunlar donanım, kağıt ve beyin cüzdanları olup aşağıda ayrıntılı bir şekilde açıklanmıştır.

I. Donanım Cüzdanlar: Bir tür şifreli USB biçimidir. Diğer tüm cüzdanlar arasında bilinen en güvenli cüzdan türü, hardware cüzdan olarak da bilinen, donanım cüzdanlarıdır. Çünkü özel anahtar, USB biçiminde olan donanımsal bir cüzdan içerisinde saklanmakta ve başka hiçbir yere kopyalanılamamaktadır. Aynı zamanda USB biçiminde olan bu donanım cüzdanı kaybedildiği ya da bozulduğu zaman başka bir donanımsal cüzdanı kişi kendi hesabına bağlayabilmektedir. Bu durum cüzdan oluşturulurken gelişigüzel yazılan 24 adet kelimenin bilinmesini ve akılda tutulmasını zorunlu kılmaktadır. Diğer yandan bu cüzdanlar sürekli internete bağlı

olmadıklarından dolayı güvenlik tehdidi sıcak cüzdan tiplerine göre daha düşüktür (Alnıaçık, 2019: 25).

II. Kâğıt Cüzdanlar: En üst düzeyde güvenlik sağlayan cüzdan türüdür. Burada kullanıcının sahip olduğu özel ve açık anahtar bir kâğıt üzerine basılmaktadır. Kağıt cüzdana kripto paranın gönderilmesi için kâğıtta yazılı olan adresin girilmesi yeterli olmaktadır. Kâğıt cüzdan içerisindeki bulunan para çekilmek istendiğinde ise bütün birikimin çekilmesi gerekmektedir. Dolayısıyla burada belli bir birikim miktarının çekilip geriye kalan miktarın bu kağıt cüzdanlar içerisinde bırakılması mümkün değildir. Bu sebepten kâğıt cüzdandan para çekme işlemi "süpürme" olarak adlandırılmaktadır (Abaday, 2018: 70).

III. Beyin Cüzdanları: Burada cüzdan tarafından üretilen, harf ve rakamdan oluşan bir seri olan özel anahtarın beyinde tutulması gerekmektedir. Bilgisayar bu harf ve rakamları senkronize ederek akılda kalabilecek bir şekilde en az 8 kelimeden oluşan özel karakterler şekline dönüştürmektedir. Dolayısıyla bu cüzdanın güvenliği oluşturulan bu uzun şifrenin akılda tutulmasına bağlıdır. Yani şifre unutulmazsa en güvenilir cüzdan tipidir (Durmuş ve Polat, 2018: 666).

2. 3. KRİPTO PARA TÜRLERİ

Kripto paralar ilk olarak 2008 yılında Satoshi Nakmoto takma adlı bir kişi veya kurum tarafından yazılan "Bitcoin: A Peer-to-Peer Electronic Cash System" adlı makale ile birlikte ortaya çıkmıştır. Böylelikle ilk kripto para birimi olarak Bitcoin piyasada kendine yer bulmuştur. Bitcoin, sanal para birimleri açısından yol gösterici olmuş ve zaman içerisinde birçok değişiklik ve düzenleme yapılarak Bitcoin alternatifi olan pek çok kripto para birimi oluşturulmuştur. Bitcoin dışında oluşturulan diğer tüm kripto para türleri, Bitcoin'den ilham alarak ve Bitcoin'e alternatif olarak ortaya çıktıklarından dolayı, Alternatif Coin anlamına gelen "Altcoin" olarak adlandırılmıştır. Bugün yüzlerce Altcoin piyasada dolaşımda bulunmakta ve her gün piyasaya yeni adını duyuran birçok Altcoin dolaşıma girmektedir. Ancak Altcoinler içerisinden özellikle Ethereum, Litecoin, Ripple gibi bazı Altcoin türleri diğerlerine göre piyasaya daha çok hakim olmaya başarmıştır. Buna karşın Altcoinlerin büyük bir kısmı mevcut kripto para birimi sistemleriyle tamamen aynı olmasından dolayı kripto para ekosistemi tarafından kabul görmemekte ve Altcoin mezarlığına gitmektedir.

Piyasaya tutunmayı başaran Altcoin'ler ise değerleri Bitcoin'e bağlı olduklarından dolayı Bitcoin piyasa değerinde yaşanan herhangi bir değişiklikten doğrudan etkilenmektedir (Aslantaş Ateş, 2016: 360).

Kripto paraların bu şekilde zamanla giderek çeşitlenmesine bağlı olarak çalışmanın bu bölümde kripto para türlerinden başlıca öne çıkanlar açıklanmıştır. Ancak burada açıklanan kripto paraların dışında piyasada yaklaşık 2500'ü aşkın kripto para türünün olduğunun da özellikle belirtilmesi gerekmektedir.

2. 3. 1. Bitcoin (BTC)

Bitcoin kripto paraların ilk ve en yaygın türüdür. Bu durum Bitcoin'in kripto paralar içerisinde ayrıntılı bir şekilde açıklanarak aydınlık kazandırılmasını gerektirmektedir. Bu bağlamda çalışmanın bu bölümünde Bitcoin'in ne olduğundan kısaca bahsedildikten sonra tarihçesine değinilmiştir. Daha sonra Bitcoin'lerin diğer kripto para birimlerindan farklı olan yönlerine aydınlık kazandırmak amacıyla Bitcoin'de transfer işleminin nasıl gerçekleştirildiği açıklanmıştır. En sonda bu kadar önemli bir yere sahip olan Bitcoin'in kullanıcılara sağladığı avantajlara ve dezavantajlara dikkat çekilmiştir.

2. 3. 1. 1. Bitcoin Nedir?

Bitcoin, güvenli şifreleme ile birleştirilmiş ve blokzincir olarak bilinen bir veri teknolojisi kullanan, dağıtılmış ağlar aracılığıyla da çevrimiçi olarak var olan kripto para birimlerinin ilki ve en popüleridir. Bitcoin, 2008 yılında Satoshi Nakamoto takma adlı bir kişi ya da grup tarafından geliştirilmiş açık kaynaklı ve yazılım tabanlı bir çevrimiçi ödeme sistemi olarak bilinmektedir. 2009 yılında ilk blok olan Genesis Bloğun yaratılmasıyla madencilik ve transfer işlemleri başlamıştır. Bitcoin'de bu transfer ya da ödeme işlemleri, BTC ya da XBT sembolü ile ifade edilirken blokzincir olarak bilinen halka açık defterlere kaydedilmektedir. İşlemler, merkezi bir depo ya da tek bir yönetici olmadan eşler arası bir ağ üzerinden gerçekleşmektedir. Diğer bir ifadeyle Bitcoin'de kişiden kişiye (P2P) doğrudan transfer yapılarak hiçbir aracıya ihtiyaç duyulmamaktadır. Merkezi olmayan bu para biriminin transfer işleminde, gönderim kaynağının ve alıcısının tespit edilmesi

oldukça güçtür. Dolayısıyla gerekli her türlü güvenlik önlemleri alınırsa hesap tamamen kişinin kendi kontrolü altında olmaktadır. (Hayes, 2017: 1309).

Bitcoin'lerle ilgili bilinmesi gereken bir diğer unsur bir Bitcoin'in en fazla yüz milyon alt birime ayrılabilmesidir. Dolayısıyla en küçük Bitcoin birimi 0,00000001'dir. Kripto para piyasasındaki bu en küçük, temel ve bölünemez para birimine Bitcoi'in kurucusu Satoshi Nakamotoya atfen Satoshi olarak isimlendirilmiştir (Gültekin, 2017: 101). Resmi olmasa bile Bitcoin topluluğu tarafından sıklıkla kullanılan başka Bitcoin birimleri de bulunmaktadır. Bu diğer Bitcoin birimleri Tablo 9'da gösterilmiştir.

Tablo 9: Bitcoin Birimleri

Bitcoin Birimi	**İsim**
1 BTC	1 Bitcoin
0. 01 BTC	1 Bitcent
0.001 BTC	1 Mbit
0. 000 001 BTC	1 Ubit
0. 000 000 01 BTC	1 Satoshi

Kaynak: (Kurt, 2018: 61).

(İda, 2017: 9)'da Bitcoin'in sahip olduğu bu özelliklerden dolayı Bitcoin'in parayı amaç olmaktan çıkararak bir araç haline getirdiğini belirterek Bitcoin'i maddeler halinde aşağıdaki gibi özetlemiştir. Bu bağlamda Bitcoin;

- Sanal bir para birimi olup herhangi bir fiziki karşılığı bulunmamaktadır.
- Bitcoin, bir ağ etkileşimidir ve herhangi bir merkezi bulunmamaktadır. Bir kişiden diğer bir kişiye dijital para transferi sağlamaktadır.
- İnternet olan herhangi bir yerden transfer işleminin gerçekleştirilmesine olanak sağlamaktadır.
- Bir aracı ya da komisyoncusu bulunmamaktadır.
- Bitcoin, açık kaynak kodla yazılmıştır ve herkese açıktır. Sistemi kullanan herkes bu sistemin sahibidir. Ancak kişisel hesaba müdahale edilememektedir.
- Tüm ülkelerde kullanılmakta ve giderek daha da yaygınlaşmaktadır.

- Kullanım koşulu ya da ön sözleşme gibi herhangi bir sınırlayıcı unsurlar ve şartlar bulunmamaktadır.
- Tüm kripto paralarda olduğu gibi Bitcoin'de madenciler tarafından üretilmektedir.
- Üretilecek toplam Bitcoin miktarı 21 milyon adet ile sınırlandırılmıştır. Yani toplam Bitcoin üretim miktarı 21 milyon'a ulaşınca Bitcoin üretimi durdurulacaktır.
- Toplam üretim miktarı belli olduğu için üretim hızını kontrol etmeye yönelik çalışmalar bulunmaktadır. Bu bağlamda Bitcoin çıkarma hızı üzerinde etkili olan ve ağdaki üretim yoğunluğuna göre belirlenen zorluk seviyesi, belli protokoller doğrultusunda sürekli olarak ayarlanmaktadır. Zorluk derecesinin ayarlanması her 1 saatte 6 blok çözülmesini garanti etmek ve bir anda tüm Bitcoin'lerin üretilmesini önlemek amacıyla yapılmaktadır.
- Her Bitcoin kullanıcısının dijital bir cüzdanı ve hesabı bulunmaktadır.
- Bitcoin'de gerçekleştirilen transferler benzersiz bir imza ile imzalanmakta ve sırasıyla madenciler tarafından kontrol edilerek doğrulanmaktadır. Bu şekilde bir Bitcoin'in iki kez kullanılması ve mükerrer ödeme engellenmiş olmaktadır.
- Bitcoin ile ürün satışı yapılması için hiçbir ek ödeme yapılmamaktadır. Bitcoin; TL, Dolar, Euro gibi birçok para birimine de dönüştürülebilmektedir.

2. 3. 1. 2. Bitcoin'in Kısa Tarihçesi

Bitcoin'in temelinin oluşturan fikirler 1985 yılında kriptoloji uzmanı olan David Chaum'un anonim dijital paradan bahsetmesiyle akıllara gelmeye başlamıştır. Daha sonra 1992 yılında "cypherpunk" adındaki bir mail grubundan Wei Dai, ilk defa arkasında merkezi bir otoritenin bulunmadığı şifreli para teorisini gündeme getirmiştir. Cypherpunk grubunun yaklaşık 700 üyesi bulunmakta ve bunlar arasında Adam Back, Nick Szaboi Phil Zimmerman, Hal Finney gibi kripto paralar açısından önemli olan isimlerde bulunmaktaydı. Bu grup anonim olan ve şifreli dijital para konusunu konuşmaya başlamıştır. Hatta gruptan bazıları kendi sistemlerini bile geliştirmeyi denemiş ancak bunlar kalıcı olmamıştır. Bu konudaki en önemli adım ise 2008 yılında atılmıştır (Abaday,2018: 19-20).

2008 yılında yaşanan küresel finansal kriz ile ülkeler ciddi bir tehlike altına girmişlerdir. ABD emlak piyasasında ortaya çıkan ve Mortgage (Konut kredisi) krizi olarak bilinen bu kriz, Amerikan ekonomisinin dünya ekonomisine yön veren bir pozisyonda ve büyüklükte olmasından dolayı tüm dünyayı olumsuz yönde etkilemiştir. Gelişmiş ekonomilerde büyüme hızı dünya ortalamalarının altında kalmış ancak gelişmekte olan Asya ekonomilerinden olan Çin ve Hindistan ekonomisi ve akabinde Rusya ekonomisi 2005 yılından itibaren dünyada en fazla büyüme gösteren ekonomilerden olmuştur. Bu durum dünya ticaret hacminde önemli daralmalara neden olmuştur. Talep daralması da bu ekonomik krizin başlamasıyla daha da gelişmiş ve 1929 krizinden sonra dünya en büyük ekonomik krizlerinden biri ile karşı karşıya kalmıştır. 1929 yılında yaşanan Büyük Buhran'ın tekrar yaşanmasından korktukları bu dönemde para birimleri büyük bir değer kaybına uğramış ve bu durum halka vergi artışları olarak yansıtılmıştır. Bu durum da halkın merkez bankasına ve hükümetlere olan güvenini büyük ölçüde sarsmıştır. Ülkelerde böyle bir ortamın hakim olduğu zamanda ise Bitcoin'in merkezi olmayan bir para birimi olarak ortaya çıkması ise manidar bir durum olarak değerlendirilmektedir. Bitcoin, Satoshi Nakamoto takma adıyla, 2008 yılında yazılan "Bitcoin: A Peer-to-Peer Electronic Cash System" yani "Bitcoin: Uçtan Uca Elektronik Ödeme Sistemi" başlıklı bir makale ile dünyaya duyurulmuştur (Uzgören, 2015: 45).

Bitcoin'in Kasım 2008'de Nakamoto tarafından kapalı bir mail grubuna yollanmış bir e-mail aracılığıyla tanıtıldığı ve 2009 yılında ilk Bitcoin yazılımının tanıtıldığı bilinmektedir. Ancak Satoshi Nakamoto'nun kim olduğu hatta bir kişi mi bir grup mu yoksa bir kurum mu olduğu da bilinmemektedir. Nakamoto'nun gönderdiği mail'in Japonyadan gönderildiği ispatlansa bile Nakamoto'nun bir Japon olup olmadığı hakkında da net bir bilgi bulunmamaktadır. Bu konuda yaşanan belirsizlikler bazı iddiaların ileri sürülmesine de neden olmuştur. Hatta isimde kullanılan kelimelerin ünlü Japon firmalarının isimlerinden alınmış harflerden oluştuğu da söylenmekte ve bu kelimelerin Japonca olduğu da bilinmektedir. (Aslantaş Ateş, 2016: 354-355).

Nakamoto'nun kimliğinde her ne kadar belirsizlik olsa da ortaya çıkardığı sistemle dünyayı etkilemeyi başarmış ve yepyeni bir sistem ortaya çıkarmıştır. Nakamotu'nun sistemi tamamıyla eşler arası bir özelliğe sahip elektronik para, çevrimiçi ödemelerin herhangi bir finans kuruluşuna bağlı olmadan doğrudan bir

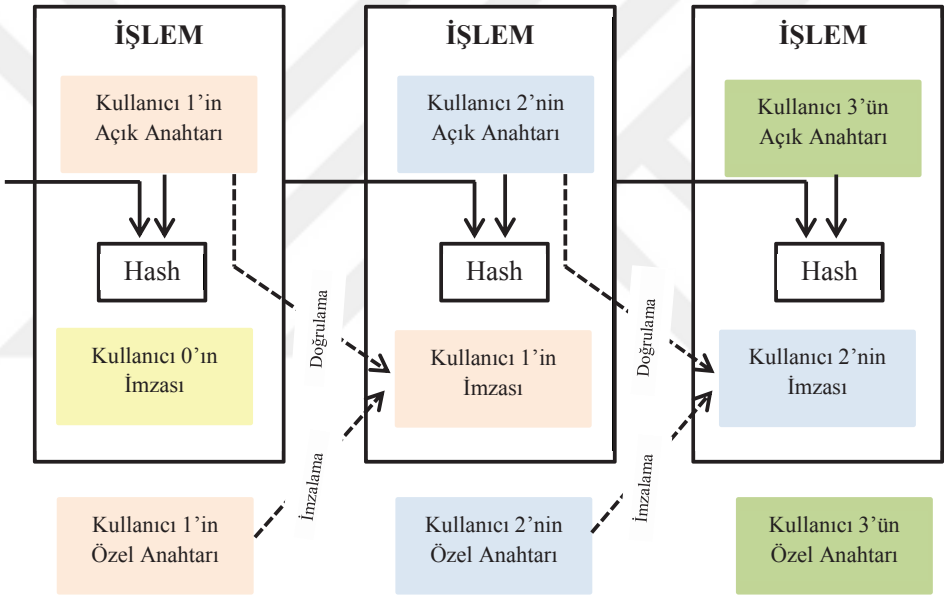
taraftan diğer tarafa aktarılması fikrine dayanmaktaydı. Sistem özellikle eşler arası ağ kullanımını aracılığıyla çifte harcama sorununu çözmeyi amaçlamaktaydı (Nakamoto, 2008: 1).

Satoshi Nakamoto tarafından önerilen bu sistem özellikle kriptoloji grubundan birçok kişinin ilgisini çekerek destek almayı başarmıştır. Bu destekle birlikte de Nakamoto Bitcoin'in ilk kaynak kodunu yazmış ve 3 Ocak 2009 tarihinde 30.000 satırlık kod, Bitcoin'in başlangıcını ilan etmiştir. Bu kodun yazılmasında ise "cypherpunk" hareketinin üyelerinden olan Hal Finney'in de destekleri bulunmaktaydı. Finney, Nakamoto'nun yazılımını ilk ilan ettiğinde, ilk Bitcoin'leri kazmayı teklif etmiştir. Bunun üzerine Nakamoto Blok 70'e ait ilk Bitcoin'i test etmek amacıyla göndermiştir. Finney, Nakamoto ile olan bu etkileşimi sonucunda "Karşımda gerçekten zeki ve samimi Japon kökenli bir genç olduğu intibasına kapıldım" cümlesini kurmuştur. Hatta bu durum Nakamoto'nun kimliğindeki gizliliğinin de etkisiyle, Bitcoin'in gerçek mucidinin Hal Finney olduğunun düşünülmesine neden olmuştur. Başta Finney olmak üzere bu şekilde birçok geliştiricinin Bitcoin'e destek sağlamasıyla Bitcoin sürekli ilerleme kat etmiştir. Hatta bu yolda 2010 yılında birkaç esnaf yerleşik para birimi yerine Bitcoin'i kabul etmeye başlamıştır. Bu doğrultuda bir Bitcoin geliştiricisinin "Evime pizza yollayan ilk kişiye 10.000 Bitcoin verebilirim" sözleriyle bir alışveriş yapmıştır. Böylelikle Bitcoin ile satın alınan ilk somut ürün pizza olmuştur. Bu sebeple ilk alışverişin Laszlo Hanyecz tarafından yapıldığı 22 Mayıs 2010 tarihi kripto para tarihinde "pizza day" olarak anılmaktadır. Bu gerçekleştirilen alışverişle birlikte de Bitcoin giderek daha çok yaygınlık kazanıp alışverişlerde kullanılmaya başlanmıştır (Aksoy, 2018: 10-12).

2. 3. 1. 3. Bitcoin Transfer İşlemi

Bitcoin transfer işlemi, herhangi bir aracı kuruluş ya da merkezi otorite olmadan eşler arası (P2P) bir ağ üzerinden gerçekleştirilmektedir. Bitcoin transferi, gönderen ve alıcı arasında e-imza ile transfer bilgisinin onaylanarak işlemin gerçekleştirildiği ve ağdaki diğer tüm Bitcoin kullanıcılarının da her transfer bilgisinin yedeğine sahip olduğu bir işlemden oluşmaktadır. Bitcoin ekosisteminde kullanıcılar; Bitcoin cüzdanı, hesap numarası benzeri uzun ve karmaşık karakterlerden oluşan ifadelerle kimliklendirilmektedir. Yeni bir Bitcoin hesabı açılmak istendiğinde

Bitcoin cüzdanı, açık kaynak kodlu bir diğer yazılım ile kimlik bilgisi üretimi yaparak kullanıcıdan şifre istenmekte ve en sonunda oluşturulan bu Bitcoin hesabı kullanıma hazır olmaktadır. Daha sonraki aşamada her Bitcoin para sahibi, bir sonraki para sahibinin yani alıcının açık anahtarını, dijital olarak imzalayarak doğrulamakta ve bunları paranın sonuna ekleyerek, parayı alıcıya aktarmaktadır. Bitcoin transfer işlemin de onaylamanın bu kadar önemli olması bir kontrol mekanizması olmasından kaynaklanmaktadır. Bu şekilde çifte harcama engellenmiş olmaktadır. (Atik vd. 2015: 250). Bitcoin transfer işlem süreci Şekil 28'de gösterilmiştir.



Kaynak: (Nakamoto, 2008: 2).

Şekil 28: Bitcoin Transfer İşlem Süreci

Bitcoin transfer işlemi aşamalar halinde şu şekilde gerçekleşmektedir. Öncelikli olarak Bitcoin para birimini alacak olan kişi adresini kullanıcıya iletmekte ve gönderimi yapacak kişi, adresi transfer işlemindeki alıcı kısmına eklemektedir. Daha sonra gönderici, kişisel kullanıcı şifresi ile gerçekleştirilen işlemi onayladıktan sonra bu işlemi diğer tüm kullanıcıların görebilmesi için yayınlayarak alıcıya gönderme işlemini tamamlamaktadır. Gerçekleştirilen transfer işlemelerinin tüm kullanıcılara duyurulmasıyla, kullanıcıları işlemi kayıt altına alarak geçmiş işlemlerine kaydetmesi ve bu şekilde gerçekleştirilen işlemler üzerinde değişiklik

yapılmasının önlenmesi amaçlanmaktadır. Bitcoin'in bu şekilde gerçekleştirilen satış işleminden sonra, paranın eski sahibinden çıkarak yeni sahibinin cüzdanına giriş kaydı, 10 dakikalık onay süreçleri sonunda otomatik olarak gerçekleşmektedir. Transfer işlemi gerçekleştikten sonra gönderilen Bitcoin üzerindeki haklar alıcı tarafa geçmektedir (Güleç, Çevik ve Bahadır, 2018: 25).

2. 3. 1. 4. Bitcoin Kullanmanın Avantajları ve Dezavantajları

Kripto para biriminin öncüsü ve en popüleri olan Bitcoin, diğer para birimlerine göre kendi içerisinde bazı avantajlar ve dezavantajlar bulundurmaktadır. Bu doğrultuda genel olarak literatür incelendiği zaman, bugünkü nihai tüketicilere sunulan alternatiflerle kıyaslandığında, dijital bir döviz ya da dijital bir para birimi aracılığıyla bir hesaptan diğerine para aktarmanın maliyetinin düşük olduğu belirtilmektedir. Ancak marjinal maliyeti neredeyse sıfır olsa bile alıcıya sağlanan marjinal faydanın marjinal maliyetten önemli ölçüde fazla olabileceği de söylenilmektedir. Ek olarak yerel hükümetlerin kurduğu para kontrollerinden kurtulmak için de Bitcoin kullanılabilmektedir. Bu durum hükümetler tarafından fazla istenmeyen bir durum olsa bile bireylere çekici gelmektedir. Dolayısıyla sağladığı avantajlar ve dezavantajlar doğrultusunda, hükümetler her ne kadar para kontrolü sağlasalar da dijital paranın bir ülkeye getirilmesi ve alım satım işlemlerinde kullanılması tamamen engellenememektedir. Bu bağlamda bu şifreli para biriminin kullanımının sağladığı avantajlar ve dezavantajların bilinerek işlem yapılması hem bireyler hem de ülke ekonomisi açısından büyük önem arz etmektedir (Dwyer, 2014: 17).

Bu bağlamda Bitcoin kullanmanın sağladığı avantajların ve dezavantajların net bir şekilde görülmesi için Tablo 10 oluşturulmuştur.

Tablo 10: Bitcoin Kullanmanın Avantajları ve Dezavantajları

Avantajlar	**Açıklama**
Düşük Enflasyon Riski	Enflayona neden olan etkenlerden biri reel para arzındaki artıştır. Tedavüldeki para arzının artması enflasyon artışına neden olmaktadır. Ancak Bitcoin'in toplam üretim miktarının 21 milyon adet olması bu durumu engellemektedir.
Düşük Çökme Riski	Reel para birimlerinin çöküşü, hükümetlere bağlı olarak yaşanan hiperenflasyondan kaynaklanmaktadır. Bitcoin sisteminin de herhangi bir hükümete bağlı olmadan işlemesi bu durumu engellemektedir.
Güvenli, Basit ve Ucuz	Bitcoin'de alıcının parasını geri talep etmesi gibi bir durum söz konusu olamayacağından, P2P sistemiyle işlemesinden ve aracı bir komisyon olmadığından dolayı güvenli ve ucuz bir işlem yapılabilmektedir.
Taşıması Kolay	Milyonlarca dolar değerindeki Bitcoin'ler küçük bir hafıza kartında bile taşınabilmektedir.
İzi Sürülemez	Bu durum suçların daha rahat işlenebilmesi, yasal olmayan maddelerin satılması gibi bazı durumlarda dezavantaj olarak da değerlendirilebilmektedir.
Dezavantajlar	**Açıklama**
Alıp Satmak Zor	Bu konuda her geçen gün gelişmeler olmakla birlikte işler, hâlâ reel para birimlerinde olduğu kadar kolay ilerlememektedir.
Kaybetme	Sahip olunan Bitcoin ya da Bitcoin cüzdanı kaybedildiği zaman bunları geri almak için kullanılabilecek herhangi bir mekanizma bulunmamaktadır.
Hâlâ Çok Yeni	Bitcoin para biriminin 2009 yılı gibi yakın bir dönemde ortaya çıkması akabinde bu tarz yeni para birimlerinin gelmesına neden olabilmektedir. Bu sistemde bazı ekliksikleri beraberinde getirmektedir.
Harcama Alanı Dar	Bitcoin'in ödeme sistemi olarak kullanıldığı alanlar oldukça sınırlı olup bugün Bitcoin sahibi olunmasındaki en büyük amaç yatırımdır
Değişken	Bitcoin'in volatilitesi oldukça yüksektir.

Kaynak: (İda, 2017: 44-45).

2. 3. 2. Altcoinler

Bitcoin, en başarılı ve ilk dijital para birimi olarak piyasada kendine yer bulmuş olsa da tek dijital para birimi değildir. Her gün yüzlercesi takas edilen farklı dijital para birimleri de bulunmaktadır. Nakamoto'nun tasarımıyla birlikte Bitcoin'in piyasada oldukça ilgi çekip değer kazanmasıyla birlikte benzer para birimleri üretmek için birçok kişi Bitcoin'i kopyalamıştır. Bitcoin'den kopyalanarak tasarlanıldığı için de bu para birimlerine genel olarak Altcoin denilmiştir. Altcoin'lere ilk örnek olarak ise Nisan 2011'de Namecoin oluşturularak Bitcoin'e ilk alternatif, piyasaya sürülmüştür. O zamandan beri Altcoin'lerden bazıları büyük bir başarı elde ederken bu başarılı coin'lerin değersiz kopyaları olan binlerce Altcoin piyasaya sürülmüştür (Ammous, 2018: 330). Çalışmanın bu bölümünde piyasada kendine yer bulmayı başarmış temel Altcoin'ler açıklanmıştır.

2. 3. 2. 1. Ethereum (ETH)

Ethereum'un Beyaz Kitabı (Ethereum White Paper) isimli çalışmanın Vitalik Buterin tarafından yayınlamasıyla birlikte Ethereum tanıtılmıştır ve kurucusu Vitalik Buterindir. Ethereum'da her hesap 20 bayt'lık bir adrese sahiptir ve bir Ethereum hesabı dört alan içermektedir. Bunlar sırasıyla her işlemin bir kez gerçekleştirilmesi için kullanılan bir sayaç, hesapta mevcut olarak bulunan ether bakiyesi, hesabın sözleşme kodu ve hesabın depolanmasıdır. Ethereum, akıllı sözleşmelerin blok tabanlı bir yazılım platformudur. Bu platform aynı zamanda Ether olarak bilinen sanal para biriminin temelini teşkil etmektedir. Ether, Ethereum blokzincirinde kullanılan kripto para birimi olup işlem ücretlerini ödemek amacıyla kullanılmaktadır. Bu bağlamda Ether, dağıtılmış uygulamaları Ethereum üzerinde çalıştırmak için kullanılan dahili kripto para yakıtı olarak değerlendirilmektedir. Burada genel olarak iki tür hesap bulunmaktadır. Bunlar özel anahtarlar tarafından kontrol edilen ve harici olarak sahip olunan hesaplar ve sözleşme kodlarıyla kontrol edilen sözleşme hesaplarıdır. Harici olarak sahip olunan bir hesabın kodu bulunmamakta ve kişiler işlemi oluşturarak ve imzalayarak harici olarak sahibi olunan bir hesaptan mesaj gönderebilmektedir. Sözleşmeli hesapta ise bu sözleşmeli hesap, her seferinde kodun aktif olduğu bir mesaj aldığında dahili depolamaya okuma, yazma ve mesajları gönderme ya da sırayla sözleşmeler oluşturmaya izin vermektedir (Buterin, 2014: 13).

Ethereum'da bir birimi göndermek için GAS'a gereksinim duyulmaktadır. GAS, Vitalik'in çalışmasından belirttiği üzere, gönderinin gideceği yere ulaşması için kullanılan bir yakıt olarak değerlendirilmektedir. GAS, bir hesaplama aracılığıyla gönderinin hızını, süresini ve buna ek olarak ne kadar harcama yapılacağını hesaplatan birime denilmektedir (Atabaş, 2018: 175).

Kripto para piyasasında Bitcoin'den sonra ikinci büyük piyasa değerine sahip olan Ethereum, blokzincir teknolojisine dayanması ve merkezi otoriteye bağlı olmaması gibi yönlerden Bitcoin'e benzerlik gösterse bile bazı yönlerden Bitcoin'den ayrılmaktadır. Bu bağlamda Bitcoin'de her bloğun oluşturulma süresi 10 dakika iken bu işlem Ethereum'da 15 saniye gibi kısa bir sürede gerçekleştirilmektedir. Bu durum Ethereum'un piyasaya çıkışındaki amaçlarından biri olarak ifade edilmektedir. Bu açıdan bakılınca da Ethereum'un Bitcoin'in işlem süresini hızlandırma amacını gerçekleştirebildiğini göstermektedir. Diğer yandan Ethereum'dan farklı olan bir doğrulama algoritmasını yani Ethash'i kullanmakta ve Ethereum madenciliğinde Bitcoin'den farklı olarak GPU olarak bilinen ekran kartlarının işlem gücü kullanılmaktadır. Aynı zamanda Bitcoin'in toplam üretim miktarının 21 milyon adet ile sınırlandırıldığı çalışmanın önceki bölümlerinde belirtilmiştir. Bu bağlamda Ethereum'da toplam üretim miktarıyla ilgili bir kısıtlama yapılmamış ancak yıllık üretim miktarı 18 milyon adetle sınırlandırılmıştır. Tüm bu farklılıklara karşın Ethereum'u Bitcoin'den ayıran en önemli özelliği akıllı sözleşmeler protokolünü kullanmasıdır (Yavuz, 2019: 20).

2. 3. 2. 2. Ripple (XRP)

Ripple, en büyük üçüncü kripto para birimi olarak piyasada kendine yer bulmayı başarmış bir Altcoin türü olup 2012 yılında piyasaya girmiştir. Kripto para piyasasından bu kadar önemli bir yere sahip bu para biriminin kurucusu ise Chris Larsendir. XRP, diğer kripto paralara göre fiyat açısından daha düşük bir seyir izlemiş olsa bile özellikle 2017 yılından itibaren yükselişi yakalamış ve bu yükseliş sayesinden Chris Larsen, dünyanın en zengin 14. kişisi olmuştur. Ripple'ın üzerinde durduğu konu, bankalar ve müşteriler arasında gerçekleştirilen ödemeleri kolaylaştırmaktır. Bu kolaylaştırma sayesinde bankaların, oldukça düşük masraflarda para transferi yapılmasına olanak sağlanmıştır. Ripple'ın işlem masrafı 0,0011 dolar

olup Bitcoin'den daha düşük bir işlem masrafına sahiptir. Ripple'da 5 ile 10 saniye arasında fon aktarılabilmekte ve gerçekleştirilen transfer işlemleri bankalar ve gönderen kişi tarafından her an kontrol edilebilmektedir. Bundan dolayı genellikle büyük firmalar ve finans hizmeti veren firmalar tarafından kullanılmaktadır. (Kesebir ve Günceler, 2019: 613).

XRP, diğer kripto para birimlerinden farklı olarak blockchain teknolojisi ile çalışmamakta dolayısıyla da Bitcoin'den neredeyse bağımsız bir yapı özellliği sergilemektedir. Merkezi olmamakla birlikte mutabakat protokolüne dayanmaktadır. Bu para biriminin üretimi ve dağıtımı Ripple labaratuvarları tarafından yönetilmektedir. Ripple'in %20'lik kısmı Ripple firmasının kurucularının elinde bulunurken %25'lik kısmına Ripple labaratuvarları sahiptir. Geriye kalan %55'lik kısım ise dağıtım yapmak amacıyla kullanılmaktadır. Burada amaç ağın büyütülmesini sağlamaktır. Ripple'da tüm defterler ilk anlardan bugüne kadar sorunsuz bir şekilde kapatılmakta ve saniyede yaklaşık 1500 işlem gerçekleşmektedir. Bu özelliğinden dolayı XRP sayesinde ödemeler çok daha hızlı gerçekleştirilebilmektedir. Aynı zamanda XRP çok nadirde olsa diğer ticari para birimleri arasında bir köprü görevi görmek ve gerçekleşebilecek herhangi bir sanal saldırıları engellemek amacıyla hizmet etmektedir (Yumuşaker, 2019: 1016-1017).

2. 3. 2. 3. Litecoin (LTC)

Litecoin, Ekim 2011 tarihinde Charles Lee tarafından duyurulmuştur. Bugün Bitcoin için önde gelen rakip kripto para birimleri arasında gösterilmektedir. Litecoin'in kurucusu Charles Lee'ye göre Litecoin, altın olarak nitelendirilen Bitcoin'e karşı, bir gümüş olarak kabul edilmiştir. Yani Lee aslında Litecoin'i duyururken Bitcoin'e bir rakip değil tamamlayıcı bir para birimi olduğunu belirtmiştir. Ancak Litecoin zaman içerisinde tahmin edildiğinden de daha büyük bir başarı göstermiş ve daima coin'ler arasında ilk sıralarda yer almayı başarmıştır. Litecoin tasarımının asıl amacı daha küçük işlemleri daha hızlı sürede gerçekleştirmektir. Bu noktada Litecoin'de diğer tüm Altcoin'lerde olduğu gibi Bitcoin'den esinlenerek tasarlanmış olsa bile Bitcoin'den bazı farklıklar sergilemektedir. Örneğin LTC, SHA-256 yerine Scrypt algoritması kullanmaktadır. Ancak bu farklıklardan en önemlisi Bitcoin'in arz edilecek toplam miktarı 21 milyon

iken bu miktar Litecoin'de 84 milyon olarak belirlenmiştir. Bu durum toplam arz miktarının Bitcoin'den yaklaşık 4 kat daha fazla olacağını göstermektedir. Aralarındaki bir diğer önemli farklılık ise Litecoin'in ortaya çıkma amacından kaynaklanmaktadır. Yani Bitcoin bloklarının işlem zamanının fazla olmasından dolayı Litecoin daha hızlı sürede işlem yapmayı amaçlamış böylelikle Bitcoin'de her işlem için yaklaşık 10 dakika gerekirken bu süre Litecoin'de yaklaşık 2,5 dakikada gerçekleşmiştir. Böylelikle bir madenci için Litecoin'i kazmak Bitcoin'i kazmaktan daha kolay olmuş ve işlem daha ucuz bir maliyetle gerçekleştirilmiştir (Bhosale ve Mavale, 2018: 134).

2. 3. 2. 4. Dash (DASH)

Eski adıyla Xcoin ya da Darkcoin olarak bilinen ancak daha sonraları suçla bağlantılı olduğu algısını değiştirmek için bu adı alan Dash, ilk olarak Ocak 2014 tarihinde lider geliştirici Evan Duffield tarafından önerilmiştir. Dash, blokzincir sistemi tarafından adem-i merkeziyetçi yönetimi serbest bırakmış ve böylelikle kripto paralar içerisinde ilk adem-i merkeziyetçi-özerk bir yapı olmuştur. Dolayısıyla Dash, gizlilik merkezli bir şifreleme para birimi olarak piyasaya tutunmuştur. Dash, anonim işlemleri yapmak için "private send" olarak adlandırılan ve anında işlemlere izin vermek için "instant send" adında bir madeni para karıştırma hizmeti kullanmaktadır (Chuen, Guo ve Wang, 2018: 35).

Dash coin'in yönetimi ve blokzincirine yeni blokların eklenmesi işlemi madenciler ve "masternode" sahipleri tarafından yapılmakta ve bu yönüyle diğer kripto paralarından ayrılmaktadır. Diğer kripto para birimlerinin çoğundan ayrıldığı en önemli nokta blok ödüllerinin sadece madencilere verilmemesidir. Burada blok ödülü madenciler ve "masternode" sahipleri arasında eşit olarak paylaşılmaktadır. Pay olarak ise ödülün %45'i madencilere ve %45'i "masternode" sahiplerine bölüştürülmektedir. Geriye kalan %10'lık kısım ise kalkınma, topluluk projeleri ve pazarlamayı finanse etmek için hazineye gönderilmektedir (Hileman ve Rauchs, 2017: 17).

Masternode sahiplerinin Dash kripto para birimini geliştirmeleri için görevleri bulunmaktadır. Bu durum "masternode" sahiplerine ayrıcalık vermektedir. Diğer yandan 1000 Dash coin'e sahip olan ve bunları sistemde muhafaza eden herkes

istediği sürece "masternode" sahibi olabilmektedir. Dash ile para işlemi yapmak için yani bu para birimini göndemek ve almak için gerekli olan süre 4 saniyedir. Bu işlemin maliyeti ise yaklaşık olarak 0.004 dolar olarak hesaplanmaktadır. Maliyetin ve sürenin bu kadar düşük olması Dash'in yaygınlık kazanmasında fazlasıyla etkili olmuştur. Aynı zamanda Bitcoin'den farklı olarak sabit kripto para birimi değildir. Bitcoin'in kullandığı node'lerden daha küçük "masternode" kullanmaktadır. Dash'in kredi kartına benzerlik gösteren "Dash Debit Card" adında kartın oluşturulması diğer kripto para birimlerinden farklılık gösterdiği bir diğer noktadır. Bu özelliğin sağladığı avantaj istenildiği herhangi bir zaman diliminde dolar, euro ya da pound çekilebilmektedir. Sahip olduğu bu farklı özellikler de Dask coin'in yaygınlaşmasını sağlamıştır (Akcan, 2018: 148-149).

2. 3. 2. 5. Monero (XMR)

Monero, işlem gören madeni paraların işlem tutarını ve ulaştığı yeri gizlemek için gizli işlemler ve gizli adresler kullanan bu doğrultuda anonim dijital nakit sağlamayı amaçlayan kripto para sistemidir (Hileman, 2017: 17). Monero, tasarımı gereği değiştirilebilir ve ucuz bir dijital değişim aracı olmayı amaçlayan bir kripto para birimidir. Üretim, depolama ve yapılan tüm işlemler XMR ağı topluluğu arasında elektronik olarak gerçekleştirilmektedir. Herhangi bir banka ya da hükümet tarafından üretilmez ve kontrol edilmezler. Dolayısıyla tamamen özerk bir yapısı bulunmaktadır. Aynı zamanda açık kaynak kodlu (PoW) bir çalışma kanıtı özelliği göstermektedir. Takip edilemezlik ve şeffaf bir blokzincire sahip BTC gibi çeşitli kripto para birimlerinden daha doğal bir gizlilik derecesine sahip olduğundan dolayı öne çıkmaktadır. Şeffaf bir blockzincir yapısına sahip olmak herkese, işlemlerin yerini izleme ve bunları sahibiyle ilişkilendirme olanağı verirken, XMR'de bu durum gerçekleşmemektedir. XMR'de işlemleri kaydetmek için Bitcoin'de olduğu gibi bir kamu defteri kullanılmakta ancak işlevselliği Bitcoin'in kodunu temel almamaktadır. Monero, tarafların adreslerini ve işlem yapılan para miktarını gizlemek için güçlü şifreleme teknikleri kullanan CryptoNote protokolüne dayanmaktadır. Yani Monero, SHA-256 ya da Scrypt yerine CryptoNote algoritması kullanmaktadır. Sergilediği bu özellikleriyle de BTC'den farklılıklar göstermektedir (Kalaitzis, 2018: 11).

CrypyoNote tamamen anonim ya da Bitcoin ile kıyaslandığında daha anonim işlemlere olanak sağlayan bir anahtar imzası kullanmaktadır. Diğer yandan halka imza olarak bilinen bir teknoloji kullanmaktadır. İşlemlerin doğru kişi ya da kişiler tarafından gönderildiğini onaylamak amacıyla da bir resmin matematiksel dengini kullanmaktadır. Ancak burada önemli olan nokta anahtar, dışarıdan bilgi olmadan o kişiyi doğrulamak için kullanılamamaktadır. Aynı zamanda her işlem yeni bir adres oluşturmakta ve buna bağlı olarak sadece gönderici nereye gittiğini bilmektedir. CryptoNote şifrelemesi, madencilerin sıradan ve normal CPU'lar kullanarak madencilik yapmasına izin verdiğinden dolayı madencilik yani üretim protokolü çok kolaylaşmaktadır. Bu sayede BTC'de olduğu gibi güçlü sistemlerde işbirliği yapmadan ya da çok para ödemeden bilgisayarlar verimli bir şekilde madencilik yapabilmektedir. Aynı zamanda Monero madenciliği kollektif olarak yapılamakta ve blokların çözümü için ortak çalışmaktadırlar. (Demartino, 2016/2018: 342).

Monero'nun temeli Bytecoin adında başka bir kripto para biriminden gelmektedir. Ancak Bytecoin'e karşı zaman içerisinde oluşan şüpheler ve piyasasına karşı gerçekleşen olumsuz yaklaşımlar Bytecoin'i çatallanmaya zorlamıştır. Bu durumla birlikte bir Bitcointalk üyesi Bytecoin'in sınırlarını keşfetmiş ve topluluğun diğer üyeleri ile birlikte bunu daha güçlü bir kodla geliştirmeye karar vermişlerdir. Sonunda 18 Nisan 2014 tarihinde Monero BitMonero adıyla bunu lanse etmişlerdir. Ancak birkaç gün sonra ekip bu adın Monero olarak kısaltılması karar vermiştir. XMR temelde beşi takma adla anonim olan 7 geliştiricisi bulunmaktadır. Bunların ise adlarının Smooth, NoodleDoodle, TacoTime, Eizh, Othe, Ricardo Spangi ve David Latapie olduğu bilinmektedir. Geliştirilen bu coin'le birlikte bazı avantajlarlar sağlanmıştır. Örneğin XMR blok sisteminde yapılan işlemler son derece hızlı işlemekte ve bir işlemi tamamlamak için 10 dakikaya ihtiyaç duyan BTC'nin aksine XMR sadece 2 dakikaya ihtiyaç duymaktadır. XMR, toplam para arzı yönünden de 31 Mayıs 2022 tarihinde XMR'nin miktarının 18,3 milyona ulaşmasını planlamıştır. Bu noktadan sonra arz artışı dakikada 0,3 Monero üretilecek ve bu miktar yılda 157788 XMR ile sınırlı olacaktır. Bu miktar her yıl azalacaktır ancak asla sıfıra ulaşmayacaktır. Yani Monero'nun piyasa arzının maksimum miktarı belli olmayıp sonsuz tutulmuştur. 2140 yılında ise hem XMR'nin hem de BTC'nin yaklaşık 21 milyon coin'i olması beklenmektedir (Kalaitzis, 2018: 12-14).

2. 3. 2. 6. IOTA

IOTA, ilk olarak 2014 yılında kavramsallaştırılmış ve daha sonra 2015 yılında David Sonstebo, Sergey Ivanchenglo, Dominik Schiener ve Dr. Serguei Popov tarafından kurulmuştur. Kurucuların birçoğu IOT ödemeleri için mevcut seçeneklerin sınırlamalarını görmeye başladığı zaman IOT odaklı bir donanım başlangıcı üzerinde çalışmışlardır. Bu sorunlara bir çözüm olarak da IOTA yaratılmıştır (Divya ve Biradar, 2015: 23823).

IOTA, teknolojiyi geliştirirken tüm geliştiricilerin birlikte çalışabilmesinin lisanssız olmasını sağlamak amacıyla herhangi bir kâr amacı gütmeyen Linux Vakfı olan IOTA Vakfı tarafından işletilmektedir. IOTA, çok yeni bir şifreli para birimi olup BC teknolojisini kullanmaması ve madencileri olmaması bakımında diğer kripto para birimlerinden ayrılmaktadır. IOTA, internetteki makineler arasında güvenli ödeme ve iletişim olanağı sağlamak amacıyla açık kaynaklı dağıtılmış bir defter özelliği göstermektedir. IOTA, BC'den farklı olarak Tangle teknoloji kullanmaktadır. Bu durum eğer bir gün temeli blokzincire dayanan paralarda sorun çıkarsa öne çıkma ihtimalini göstermektedir (İnci ve Alper, 2018: 85-85).

(De Roode, Ullah ve Havinga, 2018: 3) BC teknolojisini kullanmayan IOTA'yı BC'den üstün kılan eşsiz özelliklerini aşağıdaki gibi sıralamıştır:

- Ölçülebilirlik: IOTA, belirli bir aralıkta onaylanabilecek işlem sayısında sınırlama olmaksızın işlemelerin paralel doğrulaması aracılığıyla yüksek işlem hacmi elde edebilmektedir.
- Yerinden Yönetim: IOTA'nın madencisi bulunmamaktadır. Ağda işlem yapan her katılımcı, oy birliğine aktif olarak katılmaktadır. Bu nedenle merkezileştirilmemiştir.
- IOTA, Curl-p isimlendirilen yeni nesil üçlü hash fonksiyonunu kullanmaktadır.
- IOTA, IOT için daha uygun işlem ücreti bulunmamaktadır.

2. 3. 2. 7. Ethereum Classic

Ethereum sisteminde herhangi bir projenin geliştirilmesiyle ilgili kararlar ve işlemler DAO (Decentralizet Autonomous Organization) olarak isimlendirilen token sahiplerinin kullandığı oylarla belirlenirken DAO, sahip oldukları Tokenler aracılığıyla biriken fonlarla finasnman sağlamaktadır. Ancak bu sistemde zaman içerisinde bir açık tespit edilmiş ve oldukça büyük miktarda Ether sistemden çekilerek başka hesaplara aktarılmıştır. Bununla birlikte Ethereum topluluğu, teknik olarak yasal bir hırsızlığın nasıl ele alınacağı konusunda anlaşmazlık yaşamışlardır. Kullanıcıların büyük çoğunluğu kayıp fonları geri almak için Ethereum'un kodunu değiştirme fikrini ortaya sürmüşlerdir. Ancak bu noktada geriye kalan azınlık kısım ise Ethereum'un üçüncü taraf kişilerce müdahale edilerek değiştirilmesi gerektiğini düşünerek bu fikirlerini öne sürmüşlerdir. Bu anlaşmazlıklar Ethereum kullanıcılarının ikiye ayrılmasını beraberinde getirmiştir. Azınlık grup ise Ethereum'un hâlâ gelişen sürümü olan Ethereum Classic'i yaratmışlardır (Nebil, 2018: 48).

Ethereum ve Ethereum Classic arasında önemli farklılıklar bulunmaktadır. Öncelikli olarak her iki şifreli para birimini geliştiren ve ilginenler birbirinden farklılık göstermektedir. Ayrıca Ethereum ve Ethereum Classic değerleri bakımından birbirinden bağımsız hareket etmektedir. Farklı geliştirme yöntemleri bulunurken geliştirici kitlelerde birbirinden farklılık göstermektedir. Kullanıcıların birbirleriyle anlaşmazlıklarından kaynaklı olarak ayrılan bu iki para birimini şuan da hâlâ birbirinden bağımsız olan projeleri desteklemektedirler. Ancak birbirlerinden tamamen farklı bir yapı arz eden bu iki kripto para birimi aynı cüzdanda taşınabilmektedir (Akcan, 2018: 146).

2. 3. 2. 8. Tether (USDT)

Tether, kişileri Bitcoin'in sahip olduğu yüksek volatilite'den korumak amacıyla tasarlanmış bir Tokendir. Bu özelliğinden dolayı NuBits'i anımsatmakta ancak daha fazla para birimi tarafından desteklenmektedir. Örnek olarak TetherUSD, Amerikan Dolarına bağlıdır. NuBits'i anımsatmasına karşın USDT, NuBits'de olduğu gibi harcanabilir bir özellik sergilememektedir. Ayrıca kendi blokzincirine de sahip değildir. Daha çok günlük işlemciler veya BTC'nin volatilitesinden geçici süreliğine

de olsa uzaklaşmak isteyenler tarafından kullanılmaktadır (Demartino, 2016/2018: 339).

Diğer yandan özellikle yabancı borsalara para yatırmak ve çekmek; zor, maliyetli ve uzun bir işlem olduğundan dolayı, kripto para işlemi yapanların Tether'i yabancı borsalarda sıklıkla kullandıkları görülmektedir. İşlem yapanlar belli bir süreliğine kripto paradan çıkarak dolarda beklemek istediklerinde Tether bu kişilere istedikleri olanakları vermektedir. Ancak bu durumda bazı olumsuz durumların yaşanması da söz konusu olabilmektedir. Bu da Tether'in fiyatının dolara sabit tutulmayıp çökme riskini bünyesinde bulundurmasıdır. Bu noktada piyasa oyuncuları; bir yerden kripto paralar arasındaki akıcılığı sağladığını düşünenler ve şeffaf olmayıp tutarsız tavırlar sergilediğinden dolayı tüm kripto para ekosistemini bozduğunu düşünenler olmak üzere iki farklı gruba ayrılmaktadır. USDT hakkında olumsuz düşünceye sahip olanlar USDT'de bir çökme yaşanması durumunda geriye kalan tüm kripto paraların büyük orandan etkileneceğinden endişe duymaktadırlar (Güven ve Şahinöz, 2018: 132).

2. 3. 2. 9. Dogecoin (DOGE)

Litecoin'in en ciddi kripto para birimi olarak anılıyor olmasına karşın 2013 yılında tanıtılan Dogecoin'de en ciddiyetsiz kripto para birimi olarak anılmaktadır. Dogecoin temelde bir şaka olarak başlamış ancak piyasada ortalamadan daha uzun süre dayanma gücü sergileyerek dikkatleri üzerine çekmiştir. İnternette popüler olan Shiba Inu cinsi bir köpeğin resmi, DOGE kripto para biriminin maskotu olmuştur. DOGE'nin kurucusu olan Billy Markus'un japon ırkı bu köpekten esinlenerek Dogecoin'in ambleminde yer verdiği düşünülmektedir. DOGE, ilk benimseyenlere faydalı olması düşüncesiyle en başından yüksek ödüller sunmuş bundan dolayı da coin'in uzun süre ayakta durması beklenmemiştir. Bu bağlamda Dogecoin'in "şişir ve boşalt" coin'i olarak piyasaya sürüldüğü de sürekli tartışılmıştır. Ancak buna karşın piyasada kendini göstermeye devam etmiştir (Demartino, 2016/2018: 326).

Piyasaya şaka olarak çıkmasına karşın bu coin'e ilginin artmasının bazı sebepleri bulunmaktadır. Öncelikli olarak Scyrpt algoritmasını kullanmakta ve bundan dolayı da madencilik kolay olup herkes tarafından özel işlemcilere gereksinim duyulmadan kazı yapılabilmektedir. Ayrıca çıkarıldığı ilk zamanlarda piyasadaki

değerinde yaşanan ciddi yükselişler de oldukça etkili olmuştur. Ancak piyasaya tutunmasına karşı Dogecoin'e karşı yapılan eleştiler kesilmemiştir. Bu eleştirilerin temelinde güvenliğin tam olarak sağlanamaması gelmektedir. Bu güvensizlik, 25 Aralık 2015 tarihinde DOGE cüzdanlarına karşın gerçekleştirilen hacker saldırıları sonucunda çoğu kişinin mağdur olmasıyla birlikte artmıştır. Ancak Dogecoin Tanıtım Vakfı tarafından daha önce benzeri pek görülmemiş "Save Dogemas" adında bir uygulama başlatılmıştır. Bu uygulamayla Dogecoin sahiplerine coin aktarımı yapılmış ve yaşanan mağduriyet hafifletilmiştir. Bu durum da DOGE'ye olan güvenin ve tanınırlığın artmasında etkili olmuştur. Ayrıca 2015 yılı içerisinde değerinin Bitcoin'e yaklaşması da bu güveni iyice artırmış ve aynı yıl Kanada'nın Voncouver bölgesinde Dogecoin ATM'lerinin kurulmasıyla birlikte DOGE, kripto para piyasasında yerini sağlamlaştırmıştır (Akcan, 2018: 152-153).

2. 4. KRİPTO PARA EKONOMİSİ

Çalışmanın bu bölümünde öncelikli olarak kripto paralarda vergilendirme sisteminden bahsedilmiştir. Daha sonra kripto paraların ülkelerdeki yasal statülerine değinilmiş ve kripto paralarda arbitraj olanağı olup olmadığı açıklanmıştır. Bu başlık altında en son olarak ise kripto para borsalarına yer verilmiştir.

2. 4. 1. Kripto Paraların Vergilendirilmesi

Devletler ülkede belirli bir düzen sağlayarak halka hizmet etmek amacıyla kurulmuştur. Bu temel amacını yerine getirerek halka olan görev ve sorumluluklarını gerçekleştirebilmek için vergi toplayarak finans sağlamak devletlerin kurulduğu ilk zamanlardan beri süre gelen bir uygulama yöntemidir. Halkın gerçekleştirilecek hizmetlerin finansmanına zorunlu olarak katkı sağlaması sonucunda ise vergi hukuku geliştirilmiş ve anayasal sistemin en temel normlarından biri olmuştur. Dolayısıyla devletin halka karşın olan görevini yerine getirerek ülkede refahı sağlaması için vergi hukuku süreklilik arz etmek zorundadır. Ancak diğer tüm hukuk dallarında olduğu gibi vergi hukuku da zamanın gerektirdiği şartlara göre değiştirilmek, geliştirmek ve bu yönde devlet tarafından radikal kararlar alınmak zorundadır. Netice de gelişen teknoloji yapısıyla birlikte arz ve talep miktarında bir takım değişiklikler yaşanmaktadır. Bu yönde gelişen en son teknoloji kripto paralar olup bu şifreli para

birimlerinin vergilendirilip vergilendirilmeyeceği tartışmalarını da beraberinde getirmiştir (Kamacı ve Özden, 2019: 32).

Bu yönde kripto paraların, merkezi otoriteden bağımsız olarak üretilmesi, herhangi bir kamusal düzenlemenin bulunmaması ve anonimliği gibi etkenlerden dolayı şifreli paraların vergi kaçakçılığı ya da diğer ekonomik suçlar için elverişli olduğu yönünden tartışmalar ağırlık taşımaktadır. Bu doğrultuda özellikle Monero, yüksek düzeyde gizliliğe sahip olduğundan dolayı Amerikan Gelir idaresi gibi kurumların ekonomik ve mali suçlar üzerinde vurgu yaptığı bir konu olurken; Zcash kripto para biriminin de yapılan işlemlerin takip edilememesi özelliğinden dolayı vergi kaçakçılığı için en uygun şifreli para birimlerinden biri olduğu söylenilmektedir. Kripto para birimlerinin yeni bir vergi sığınağı alternatifine dönüşmesinde, devletlerin geleneksel vergi sığınağına karşı yürüttükleri mücadeledeki artan kararlılıklarına bağlı olarak, eski tür vergi sığınaklarına para aktarmanın giderek güçleşmesi de belirleyici bir unsur olmuştur. Ayrıca devletlerin bu süreç içerisinde bankalar ya da finansal kurumlar gibi üçüncü tarafları, kıyı ötesi işlemlerde bilgi açıklamada yükümlü kılması ve bu tür işlemler olduğunda stopaj yoluyla vergi kesme sorumluluğu yüklemesi geleneksel vergi sığınaklarının çekiciliğini azaltırken kripto paralarda bu çekiciliği artırmaktadır. Özellikle de krizlerin yaşandığı dönemlerde ülkelerde kripto para birimlerinin kullanım oranlarında artış yaşanması da bu durumu destekleyen bir unsur olarak gösterilmektedir (Şahin, 2019: 176).

Kripto paralara yönelik yapılan bu tartışmaların akabinde ise kişilerin ve kurumların haklarının korunması gerektiği ve devletler için kripto para birimlerinin önemli bir gelir kaynağı olabileceği düşüncelerini getirmiştir. Bu düşünceler kripto paraların bir vergilendirme sistemine tâbi tutulması fikrini değerlendirmelerine neden olmuştur. Bu hususlar için tüm ülkeler açısından tanımlanmış bir metod bulunmamaktadır. Ancak kripto paralardan kazanç elde edenlerin vergi konusuna tâbi tutulması için kazancının konusunun da belirlenmesi gerekmektedir. Bu doğrultuda Gelir idaresi tarafından kripto paraların ilk türü olan Bitcoin örnekleminde Bitcoin'in ilk olarak bir "emtia" ikinci olarak bir "menkul kıymet" ve son olarak " para" olarak değerlendirmesi hususunda vergiye dahil edilebileceğini belirtmiştir (Akiz, 2019: 9-10).

I. Emtia: TDK sözlüğü'nde emtia "ticaret, mal" olarak tanımlanmakta ve kelimenin kökeni Arapça meta sözcüğünden gelmektedir. Türkçe'de ticari bir alım

satıma konu olan bütün mallar emtia olarak ifade edilmektedir. Petrol, altın, gümüş, bakır, metal, mineral gibi değerli madenlerin yanı sıra arpa, buğday gibi temel gıda maddeleri ve bir başka ürünün hammaddesi olarak kullanılabilen kahve, şeker, kömür gibi ürünler de emtia olarak isimlendirilmektedir. Ayrıca emtia'ların bir diğer özelliği borsada yatırım aracı olarak işlem görebilmesidir. Emtia'ların işlem gördüğü borsalara ise "emtia borsası" denilmektedir. Bu yönden Türkiye Odalar ve Borsalar Birliği'ne bağlı toplam 113 adet "emtia borsası" bulunmaktadır. Diğer yandan muhasebede işletmenin üretim ve alım-satım işlemlerine konu olan varlıklar da bir emtia olarak değerlendirmektedir. Bu doğrultuda kripto paraların altına benzemesine bağlı olarak emtia olarak değerlendirilebileceğini savunanlar bulunmaktadır. Diğer yandan kripto paralar, madenciliğe dayanan bir yapı sergilediğinde dolayı eğer bu madencilik faaliyeti sonunda elde edilen kripto paralar yasal otoriteler tarafından emtia olarak kabul edilirse alım-satım işlemlerinin bir karşılığı olarak KDV vergisinin uygulanması gerekmektedir. Aynı zamanda emtia olarak kabul edildiği her durumda bir gelir elde edildiğinden dolayı gelir ve kurumlar vergisine tâbi tutulması gerekmektedir. (Yalçın, 2019: 108-111).

II. Menkul Kıymet: Orta ve uzun vadede bir yatırım aracı olarak kullanılan ortaklık ya da alacaklılık hakkı sağlayan kıymetli evraktır. 6102 sayılı Türk Ticaret Kanunu'nun 7. Bölümünde menkul kıymetler yer alıp bunlar; pay senetleri, intifa senetleri, borçlanma senetlerini alma ve değiştirme hakkını içeren üç farklı kısımdan oluşmaktadır. Mezkûr kanunun ilgili bölümünde, menkul kıymet kapsamında ortaklık hakkı tanıyan pay senetlerinin ve alacak hakkı tanıyan intifa senetlerinin olduğu, bu bağlamda şifreli para birimlerinin menkul kıymet olarak düşünülemeyeceği görülmektedir. Sadece kripto paraların bir araya getirilmesiyle bir varlığa dayanan menkul kıymet oluşturulması halinde menkul kıymet olarak değerlendirilebileceği düşünülmektedir. Ancak bu durumda dahi kripto paralar tam olarak menkul kıymet kabul edilememekte, sadece bu paraların yer aldığı paylar menkul kıymet olarak tanımlanabilmektedir. Bu açıklamalarla birlikte eğer kripto paralar bir menkul kıymet ya da sermaye piyasası aracı olarak değerlendirilirse 193 sayılı Gelir Vergisi Kanunu'nun mükerrer 80. Maddesi gereği bir değer artış kazancı kapsamında vergilendirmesi gerekmektedir. Mezkûr kanun maddesinin 1. Fıkrasında ise bu menkul kıymetlerin elden çıkarılması durumunda elde edilen kazançların değer artış kazancı olarak vergilendirileceği ve bu fıkra gereği 01.01.2019 tarihi itibariyle 305

Seri Numaralı Genel Tebliğde belirtilen 14.800 TL'lik istisna tutarından yararlanılacağı belirtilmiştir (Kızıl, 2019: 185-186).

III. Para: Bir cismin ya da nesnenin para olarak değerlendirilmesi durumunda taşıması gereken bazı özellikler bulunması gerekmektedir. Bunlar çalışmanın birinci bölümünde ayrıntılı bir şekilde açıklanmıştır. Bu özellikler kapsamında eğer kripto paralar para olarak kabul edilirse 213 sayılı Vergi Usul Kanunu'nun 289. Maddesi hükümleri uyarınca yazılı olmayan veyahut yazılı olup da kendi ölçüleriyle değerlendirilmesine imkân bulunmayan iktisadi kıymetlerin varsa borsa rayici yoksa mukayyet değerleri ise o da yoksa emsal bedeliyle değerlendirilmesi gerekmektedir. Bu bağlamda Türkiye'de yabancı para borsası bulunmadığı göz önünde bulundurulursa mukayyet değer ile değerlendirilmesi gerekmektedir. Bundan dolayı kripto paranın, piyasa arz ve talep miktarlarına göre belirlenen değerinde ortaya çıkan bir yükseliş ya da düşüş için değerleme yapılmasına gerek duyulmamaktadır (Akiz, 2019: 10-11).

Yapılan bu açıklamalar doğrultusunda vergilendirmede ülkelerin kripto paraları ne olarak değerlendirdiği önemli bir unsurdur. Çünkü ülkelerin kripto paralara yönelik uyguladıkları vergi politikaları bu bağlamda birbirinden farklılık göstermektedir. Tablo 11'de bazı ülkelerin kripto paraları vergilendirme durumları gösterilmiştir.

Tablo 11: Seçilmiş Ülkelerin Kripto Paraları Vergilendirme Durumları

Ülkeler	Açıklama
ABD	Kripto parayı emtia olarak tanımlamaktadır. Aynı zamanda çalışanlara veya hizmet alınan kişilere Bitcoin ile ödeme yapıldığı durumda bu bir gelir sayılıp gelir vergisine tâbi tutulmaktadır. Ancak ABD'de para hareketlerinin ve gelir kaynağının vergi idaresi tarafından sorgulanabilmesi kripto paraların vergilendirilmesinde etkili olmaktadır.
Almanya	Kripto para birimlerini yabancı ülke paraları ile aynı statüde kabul etmekte dolayısıyla kripto parayı para olarak değerlendirmektedir. Ancak 800 Euro'yu geçmeyen değer artış kazancı vergiden muaf tutulmaktadır. Bir yıldan daha kısa süreli olarak elde tutulan Bitcoin %25 oranında gelir vergisini tabi tutulmuştur.

Avustralya	Bitcoin'i bir para veya döviz olarak değil değer artış kazancı elde edilebilecek bir varlık olarak değerlendirilmektedir. Bitcoin, kişisel çıkar amacıyla kullanılan bir mal ya da hizmet ödenmesinde kullanıldığı ve gerçekleştirilen işlemin değeri 10.000 AUD'den daha düşük olması durumunda vergiden muaf tutulmaktadır.
Brezilya	Dijital para birimleri, finansal bir varlık olarak değerlendirilmekte ve satış anında %15'lik sermaye kazançları vergisine tabi tutulmaktadır. Ayrıca 35.000 realden düşük bir değerle satıldığında vergiye tâbi tutulmaktadır. 1000 realden daha fazla dijital para tutan her kişi yıl sonunda kesin tutarı beyan etmek zorundadır.
Bulgaristan	Bulgaristan Ulusal Rezerv Ajansı, dijital para birimlerinin satışını, Brezilya da olduğu gibi finansal varlıkların kapsamında gelir olarak değerlendirmektedir. Bu doğrultuda ülkede %10'luk sermaye kazancı vergisi geçerli olmaktadır.
Finlandiya	Bitcoin'e bir sermaye kazanç vergisi koyulmasına karşın madencilikle üretilen Bitcoin, düzenli gelir olarak değerlendirilip vergilendirilmiştir. 2014 yılında ise bir emtia olarak değerlendirilip bu konuda vergilendirme üzerine düşünülmüştür. Bu yüzden Finlandiya şimdiye kadar kripto parayı vergilendirme yönünden net bir tavır sergilememiştir.
Hollanda	Bitcoin, ülke içerisinde diğer para birimleri nasıl vergilendiriliyorsa aynı şekilde vergilendirilmektedir.
Japonya	Ülkede emtia olarak değerlendirilen kripto parayı gelir ve sermaye kazançları vergisiyle vergilendirmektedir.
Kanada	Ülkede emtia olarak değerlendirilen kripto para birimlerine, mal ve hizmet için uygulanan statü geçerli kılınmıştır. Ticari kazanç veya değer artış kazancı olarak değerlendirilip vergilendirmektedir.
Slovenya	Borsalara ve diğer topluluk üyelerine Bitcoin satılma işlemi vergilendirmezken Bitcoin, ülke içerisinde diğer para birimleri her nasıl gelir vergisine tâbi tutuluyorsa aynı şekilde vergilendirmektedir. Ayrıca vergilendirme tutarı işlem anında BTC/EUR kuruna göre hesaplanmaktadır.

Kaynak: (Günay ve Kargı, 2018: 70; Prypto, 2016/2018: 125-127).

2. 4. 2. Ülkelerin Kripto Paralara Yaklaşımı

Dünya üzerinde kripto paraların popülerliği, 2009 yılında Bitcoin'in kendini göstermesiyle birlikte, giderek daha da artmaktadır. Türkiye'de de kripto paraların kullanımı avukatlık, danışmanlık ücretleri gibi çeşitli sektörlerde ve alışveriş merkezleri, havaalanı gibi farklı yerlerde görülmektedir. Türkiye bu yönde Bitcoin ATM'sini İstanbul Atatürk Havalimanı'nda açmış ve bu konuda dünyadaki ilkler arasında yer almayı başarmıştır. Ayrıca Türk Lirası ile Bitcoin alıp satan sanal borsalar bulunurken bazı işverenlerin çalışanlarına Bitcoin ile ödeme yaptığı da görülmüştür. Bu şekilde hayatın her alanına hakim olan kripto paralar üzerinde ise ülkeler bir uzlaşıya varamamıştır. Bu doğrultuda bazı ülkeler kripto paraların kullanımı desteklerken gerekli düzenlemeleri yaparak riskleri minimize etmeye çalışmışlardır. Bazı ülkeler ise riskleri öne çıkararak kripto paraların alım satım işlemlerinin yasalara ve düzenlemeler aykırı olduğunu dile getirmişlerdir (Dizkırıcı ve Gökgöz, 2018: 98-99). Bu doğrultuda ülkelerin kripto paralara yaklaşımı ve bu paraların ülkedeki yasal statüleri Tablo 12'de kısaca açıklanarak bu konuya aydınlık kazandırılmaya çalışılmıştır.

Tablo 12: Kripto Paraların Ülkelerdeki Yasal Statüsü

Ülkeler	Yasal Statü	Açıklama
ABD	Yasal	ABD "önce yap sonra af dile" felsefesi doğrultusunda hareket eden bir ülke olup ülkede girişimcilik oldukça gelişmiştir. Bu doğrultu da Amerika kripto paralara karşı dostane bir yaklaşım sergilemektedir. ABD hazinesi 2013 yılı içerisinde kripto paraların ilki ve en popüleri olan Bitcoin'i sanal bir para birimi olarak sınıflandırmıştır. Kısaca ülkede Bitcoin bir para birimi olarak kabul edilmese bile parasal hizmet sektörünün bir parçası olarak görülmektedir.
Almanya	Yasa Dışı Değil	Kripto paralar, yasal açıdan bağlayıcı mali araçlardır.
Avrupa Birliği	Yasa Dışı Değil	2015 yılında Bitcoin bir emtia olmaktan ziyade bir para birimi haline getirilmiştir.
Avustralya	Yasal	Bitcoin konusunda en dostane tavrı sergilen ülkelerden biridir. Ülkede Bitcoin almak, satmak, madencilik yapmak serbesttir. Ayrıca Bitcoin ile yapılan işlemleri takas olarak tanımlanmıştır.
Belçika	Yasa Dışı Değil	Bitcoin ile ilgili herhangi bir olumlu veya olumsuz düzenleme bulunmamaktadır.

Birleşik Krallık	Yasal	Bitcoin'i özel para olarak sınıflandırıp Bitcoin ile yapılan alışverişlere KDV uygulanmaktadır.
Çin	Yasa Dışı Değil	Bitcoin'e karşı en düşmanca tavrı sergilemesine karşın Bitcoin'in en popüler olduğu ülkedir. Her ne kadar bankalar gibi finansal firmalar Bitcoin'le işlem yapmada sınırlamalar yapsa bile insanlar ve şirket ülkede Bitcoin alıp satabilmekte ve ticaret yapabilmektedir.
Danimarka	Yasa Dışı Değil	Nakit para kullanımını kaldırmak istediğinden dolayı Bitcoin ve itibari dijital parayı günlük hayatın içerisine katmaya çalışmaktadır.
Estonya	Yasal	Özellikle blockchain konusunda ileri gelen ülkelerden biridir. Bu yönde blockchain'i sağlık ve bankacılık gibi birçok alanda kullanmakla birlikte vatandaşlarına blockchain tabanlı ilk elektronik oylama sistemini getirmiştir.
Fransa	Yasa Dışı Değil	Belçika'da olduğu gibi kripto paralara karşı tavırsız kalan ülkelerden biridir.
Güney Kore	Yasal	Bitcoin'i bir ödeme yöntemi olarak kabul ederken ülkede kripto paraların yaygınlığı sürekli artış eğilimi göstermektedir.
Hollanda	Yasal	Blockchain teknolojisini yaygın bir şekilde kullanmakla birlikte ülkede Bitcoin kullanan şirket sayısı 100'ü geçmektedir.
İzlanda	Yasal	2008 finansal krizinden en çok etkilenen ülkelerden biri de İzlanda olup ülkeden para çıkışını engellemek amacıyla birçok düzenleme uygulanmıştır. Bu bağlamda İzlanda Bitcoin'i de bir tehlike olarak görüp Bitcoin kullanımını tamamen yasaklamıştır. Ancak 2017 yılında yapılan bir düzenleme ile birlikte bu konuda düzenlemeler yapılmıştır.
İsrail	Yasa Dışı Değil	Kripto paraları düzenlemeye yönelik herhangi bir uygulama ya da politika bulunmamaktadır.
İsveç	Yasal	Danimarka'da olduğu gibi nakit kullanımını kaldırmayı amaçlayarak Bitcoin'i ödeme metodu olarak yasallaştırmıştır.
İsviçre	Yasal	İsviçre Federal Demiryolları bilet makinelerinde Bitcoin satılmaktadır.
Jamaika	Yasal	Ülkenin MB'sı kripto paranın kullanılması ve bu yönde fırsatların yaratılması konusunda destekte bulunmaktadır.
Japonya	Yasal	Dijital para birimlerini resmen para olarak tanımıştır.
Kanada	Yasal	Kripto paralar konusunda dostane bir tavır içerisinde bulunmaktadır. Ayrıca Bitcoin'i bir emtia olarak tanımlamakta ve sadece kara para aklama operasyonlarındaki kullanımına yönelik mücadele vermektedir.

Meksika	Yasal	"Fintech Yasası" ile düzenlenerek kripto para yasalaştırılmıştır.
Rusya	Yasa Dışı Değil	Rus Ekonomi Bakanlığı ilk başlarda tüm kripto paraları yasa dışı olarak ilan edecek bir kanun çıkarmayı plandıklarını açıklamıştı. Rusya'nın devlet başkanı Putin'de bu yönde kripto paraların kanun dışı aktiviteleri finanse ettiğini açıklayarak bu para birimlerinin tehlikeli olduğunu düşünmüştü. Ancak kısa bir süre sonra Putin, Ethereum'un kurucusu Vitalik Buterin ile bir araya gelmiş ve Buterin'e Rusya'ya özel olacak bir dijital paranın nasıl yapılabileceğini sorusunu yöneltmesiyle birlikte kripto paralara karşı ılımlı bir tavır sergilenmiştir.
Tayland	Yasal	Tayland Bankası, 2016 yılında Bitcoin'in yasa dışı olmadığını ancak bu konuda temkinli hareket edilmesi gerektiğini açıklamıştır.
Türkiye	Yasa Dışı Değil	Türkiye bu konuda ikiye ayrılmıştır. Dönemin başbakan yardımcısı ve ekonomi bakanı, balon ve saadet zinciri benzetmesi yaparken cumhurbaşkanının ekonomi başdanışmanı Cemil Ertem bunun bir saadet zinciri olmadığını ancak regülasyonlar gelene kadar spekülatif bir yatırım aracı olduğunu belirtmiştir. Bu ikilemden dolayı bugün ülkede bu konuda sürekli araştırmalar yapılmakla birlikte ülkede Bitcoin alımı, madenciliği veya kullanımı yasak değildir.
Venezuela	Yasa Dışı Değil	2014'de Suudi Arabistan, İran'ın güçlenmesini engellemek ve ABD'nin kaya gazı ve petrol üretimini zayıflatmak amacıyla petrol üretimini önemli ölçüde artırmış ve petrol fiyatlarının düşmesine neden olmuştur. Yaşanan bu durumdan da en çok etkilenenlerden biri Venezuela olmuştur. Ülkenin geliri bir anda düşmüş ve yıllık enflasyon oranları %700 oranlarına kadar yükselmiştir. 2017 yılında ise Venezuela Bolivarı'nın değeri o kadar düşmüştür ki insanlar ufacık bir şey almak için bile çuvallarla parayı hiç saymadan vermeye tüccarla da saymadan almaya başlamıştır. Ülke içerisinde böylesine derin bir ekonomik buhrandan kurtulmak isteyen kişiler ise yeni arayışlara başlamış ve ellerindeki değersiz Bolivar'ları Bitcoin'e dönüştürerek hayatlarını geçirmeye başlamışlardır. Bu durum ülkenin genelinde hâkim olmuş ve bu bağlamda gündelik hayatta Bitcoin'i kullanan ilk ülke Venezuela olmuştur.
Yunanistan	Yasa Dışı Değil	Kripto paralara yönelik herhangi bir mevzuat bulunmamaktadır.

Kaynak: (Aba Şenbayram, 2019: 85-86; Aksoy, 2018: 68-77).

2. 4. 3. Kripto Paralarda Arbitraj Uygulaması

Arbitraj; döviz, menkul değer, mal ya da üretim faktörü gibi ekonomik varlıkların eş zamanlı fiyat farklılıklarından faydalanmak amacıyla yine eş zamanlı olarak alınıp satılması şeklinde yapılan işlemlere denilmektedir. Başka bir tanıma göre arbitraj, farklı piyasalarda aynı varlıkların aynı anda oluşan fiyat farklılıklarından yaralanmak amacıyla varlığın fiyatının düşük olduğu piyasadan alınıp, yüksek olduğu piyasada satılarak kâr elde etme işlemidir. Arbitrajda en temel amaç fiyat farklılıklarından yararlanarak risksiz kazanç elde etmektir. Arbitrajda bu şekilde herhangi bir risk üstlenmeden, eş zamanlı fiyat farklılıklarından bir kazanç sağlanması arbitrajı spekülasyondan ayıran en temel özelliktir. Bunun en belirgin örneği döviz arbitrajıdır (Taçali, 2008: 40).

Tanımdan da anlaşılacağı üzere arbitrajda en önemli unsur kısa sürede işlemin gerçekleştirilmesidir. Bu bağlamda kripto paraların kullanılarak arbitraj yapılması çok fazla istenilmemektedir. Çünkü kripto para birimlerinin bir borsadan başka bir borsaya transferi belirli bir zaman almaktadır. Oysa arbitraj ile kâr elde edebilmenin temel şartı farklı ülkelerde ya da yerlerde oluşan fiyat farklılıklarından anlık veya çok kısa sürede yararlanmaktır. Bitcoin ile bir borsadan diğer borsaya transfer işlemini gerçekleştirmek en az 20 dakika süre alırken bu süre 1 saate kadar uzayabilmektedir. Bu süre içerisinde ise fiyatlarda bir düşme yaşanıp beklenen kârda bir azalma olabilmektedir. Bu doğrultuda kâr beklenirken tam tersi zarar da edilebileceğinden dolayı Bitcoin ile arbitraj yapılması önerilmemektedir. Ancak bu para birimleriyle arbitraj işlemi yapılmak istenirse, Altcoin'lerde daha hızlı para transferi yapılabilmesinin etkisiyle, Altcoin'lerde yapılması genel olarak önerilmektedir (Erkuş ve Gümüş, 2019: 46).

Arbitraj'da hız çok önemli olduğundan dolayı en yoğun olduğu zamanda bile 5 dakika gibi kısa bir süre içerisinde transfer işlemini gerçekleştirebilen Dash gibi Altcoin'lere yönelmek stratejik bir yaklaşım olmaktadır. Bugün itibariyle hızlı transfer yapılabilen yüzlerce coin bulunmaktadır. Bu doğrultuda en stratejik seçimi yapmak için piyasanın sürekli takip edilmesi gerekmektedir. Transfer hızı ve işlem hacmine bakılarak arbitraj yapılacak coin belirlendikten sonra mutlaka kripto para borsalarına üye olunması gerekmektedir. Bu doğrultuda sağlanan kâr oranını artırmak için ikiden fazla sitenin kullanılması önerilmektedir. Kullanılacak sitenin seçiminde

ise fazla sayıda coin içeren ve işlem hacminin yüksek olduğu sitelerin seçilmesine dikkat edilmesi gerekmektedir. Genellikle işlem hacminin en yüksek olduğu sitelerde satış işlemi, işlem hacminin daha düşük olduğu sitelerde ise düşük fiyattan alış yapmak daha kolay olmaktadır. Dolayısıyla iki farklı siteden alış emri girmek düşük fiyattan alım şansını artırmaktadır. Burada bir kayba uğramamak için de arbitraj işlemini gerçekleştirdikten sonra takas sitelerinde kripto para bırakılmamalı ve kişinin sadece kendi kontrolünde olan cüzdana aktarılmalıdır (Kurt, 2018: 139-140).

2. 4. 4. Kripto Para Borsaları

Bir kripto para elde edilmek istenildiği zaman bunun en kolay yolu bir kripto para borsasından ulusal paralarla ödemeyi gerçekleştirerek bu kripto parayı satın almaktır. Bugün merkezi ve merkezi olmayan borsalar olmak üzere iki tip kripto para borsası bulunmaktadır. Bunlardan kullanıcıların borsaya gönderdikleri kripto paraları cüzdanlarında ya da sistemlerinde sakladıkları ve kullanıcıların bu borsalara göndermiş oldukları coin'lerin kullanıcısı olmadıkları borsa tipine merkezi borsalar denilmektedir. Merkezi borsalarda kullanıcılar hesaplarındaki paralardan tamamen kendiler sorumlu tutulmaktadır. Ancak bu borsa tipleri güvenlik açısında riskler içerdiklerinden ve hükümetlerin isteklerine bağlı olarak kullanıcıların hesapları askıya alınabildiğinden dolayı çok fazla tercih edilmemektedir. Merkezi olmayan borsalar ise kullanıcıların fonlarını saklamadan işlem yaptıkları borsalardır. Bu borsalarda merkezi borsalardan farklı olarak kullanıcıların sahip oldukları paraların kontrolü tamamen kullanıcının kendisine ait olmaktadır. Güvenlik açısında kıyaslandığında ise oldukça tedbirli borsalar olduğu görülmektedir. Aynı zamanda herhangi bir hükümete veya merkeze bağlı olmadıklarından dolayı kullanıcıların hesaplarının askıya alınması söz konusu olmamaktadır (Çiydem ve Selçuk, 2019: 17).

Bitcoin'in 2009 yılında ortaya çıkmasıyla birlikte kripto paraların önemi artmış ve bu paraların alım satım işlemlerini gerçekleştirmek için kripto para borsalarına ihtiyaç duyulmaya başlanmıştur. Bu doğrultuda Bitcoin alım ve satımının gerçekleştirilebileceği ilk borsa olan Bitcoin Market 6 Şubat 2010 tarihinde kurulmuştur. Gerçekleştirilen bu ilk borsa girişimiyle birlikte de borsa sayılarında sürekli artış yaşanmış hatta bazıları yüksek işlem hacmine ulaşmayı başarmıştır. Bu büyük ilgiyle birlikte düzenin sağlanabilmesi için kripto para borsaların da bazı

düzenler ve kurallar oluşturulmuştur. Örneğin; kripto para borsaları, resmi tatillerde dahil olmak üzere 7 gün 24 saat açık olup kesintisiz bir şekilde işlemektedir. Ayrıca bu borsalarda işlem görebilmek için üye olmak gerekmektedir. Genellikle üyelik sırasında kişisel bilgiler için kimlik belgesi veya pasaport gibi resmi belgeler istenilmektedir. Ancak bu durum bir yandan anonim işlem yapılmasını engellerken bir yandan da transfer işlemlerinin izlenmesini kolaylaştırmaktadır. Kripto para borsalarında yapılan işlem hacmine bağlı olarak komisyon ücreti alınırken bu oranın borsaya göre değiştiğinin de bilinmesi gerekmektedir. Aynı zamanda bu komisyon ücretinin dışında işlemlerin onaylanmasına olanak sağlayan madencilere bağışta gerçekleştirilebilmektedir. Böylelikle gönüllü olarak verilen bu tutar sayesinde işlem önceliğinde bir avantaj sağlanabilmektedir (Koçoğlu, Çevik ve Tanrıöven, 2016: 82).

Kripto para borsaları bulundukları ülkenin yasaları doğrultusunda hareket edebilmektedirler. Ancak şuan tüm dünyada hizmet verebilecek tek bir borsa bulunmamaktadır. Farklı ülkeler için farklı borsalar hizmet vermekte ve verdikleri bu hizmet karşılığında farklı oranlarda hizmet bedeli almaktadırlar. Birçok borsa da kendi içerisinde lehdar ve keşideciyi karşı karşıya getirmektedir (Çeker, 2018: 19). Bugün dünyada hizmet veren kripto para borsalarının başında Bitstamp, Binance, KuCoin, Coinbase, Bitfinex, Kraken, Cex.io, ShapeShift, Popniex gelmektedir. (Özden, 2019: 30). Dünya üzerinde bu şekilde önde gelen kripto para borsalarına Tablo 13'de yer verilmiştir.

Tablo 13: Dünya'da Önde Gelen Kripto Para Borsaları

Kripto Para Borsası	Borsanın Özellikleri
Coinbase	Dünyanın en popüler aracı ve ticaret platformlarından biridir. Kullanıcılar Android ve İPhone'da bulunan dijital bir cüzdan aracılığıyla bu borsadana Bitcoin, Bitcoin Cash, Ethereum ve Litecoin satın alabilmekte ve şirketin yan kuruluşu olan Coinbase Pro üzerinden ticaret yapabilmektedirler. Bu borsada, bugün ABD, Birleşik Krallık, Kanada, Singapur gibi birçok ülkede işlem yapılabilmektedir.
CEX.IO	Kullanıcıların kripto paralarla ve fiat para ile ticaret yapabilmektedir. Site güvenli olup şifreli soğuk depolarda saklanmaktadır. Tüm dünyada kullanılmakla birlikte her ülkede farklılık gösteren kısıtlamalar bulunmaktadır.

LocalBitcoins	P2P Bitcoin borsası olup alıcılar ve satıcılar bir emanetçi gibi çalışmaktadır. Kimlik doğrulaması ve kişisel bilgiler gerektiren borsaların aksine kişinin adı satın aldığı Bitcoin'e bağlanmamaktadır. Ayrıca yatırımcılar kendi fiyatlarını kendileri belirlemektedir. Satıcı, işlemin tamamlandığını doğruladıktan sonra fonlar serbest bırakılmaktadır. Alıcı satıcı arasındaki anlaşmazlığı çözmek için destek ve çatışma çözme ekibi bulunmaktadır. Almanya ve New York eyaleti dışında neredeyse her ülkede kullanılmaktadır.
Bitfinex	İşlem hacmi açısından istikrarlı olan en iyi borsalar arasında gösterilmektedir. Daha çok orta ve yüksek derecede uzmanlaşmış tüccarlara hitap etmektedir. Çeşitli coin'ler, alım satım eşleştirmeleri ve opsiyonları sunmaktadır. ABD Doları işlem hacmi açısında fazlasıyla yüksek likiditeye sahiptir. Para yatırım işlemleri için ücret alınmamaktadır. Fakat banka transferleri, yatırım miktarının %0.1'i veya 20 dolardan daha büyük şeklinde ücretlendirilmektedir.
Bitstamp	AB merkezli olarak 2011 yılında kurulmuştur. Londra, Newyork ve Lüksemburg'ta ofisleri bulunmaktadır. Ayrıca Lüksemburg Finans Bakanlığı tarafından lisanslandırılmış bir kripto para borsasıdır. Mevcut olan kripto para birimleri arasında Bitcoin, Litecoin, Ripple, Ethereum, Bitcoin Cash yer almaktadır. İki aşamalı kimlik doğrulama ve tamamen soğuk depolama gibi güvenlik hizmetleri sunmakta ve çok dilli kullanıcı ara yüzü sunmaktadır.
Kraken	İlk kripto para borsası olarak 2011 yılında kurulan küresel bir Bitcoin borsasıdır. San Francisco merkezli olup ABD, Kanada, Japonya ve Avrupa'ya hizmet sağlamaktadır. Kraken aynı zamanda ilk kripto para bankasının da ortaklarından olup 20'den fazla kripto paranın işlem görmektedir. Bunlar arasında Bitcoin, Ethereum, Monero ve Eos başta gelmekle birlikte Euro, ABD Doları, Kanada Doları, İngiliz Sterlini ve Japon Yeni arasında işlem yapılmasına izin vermektedir. Kraken ücretleri ise %0 oranı kadar düşükken bu oran sonraki süreçte yapılan ticarete bağlı olarak değişmektedir.

Kaynak: (Yakut, 2018: 164-173; http 1; http 2).

Tüm dünya üzerinde olduğu gibi Türkiye'de de kripto paralara olan ilgide sürekli artışlar yaşanmış ve bu para birimlerden bir kazanç sağlama ya da kâr elde etme düşüncesiyle girişimlerin ilgisini çekmeyi başarmıştır. Dolayısıyla Türkiye'de de kripto para borsalarına olan ihtiyaç artmış ve bu yönde bazı adımlar atılıp sürekli gelişme göstermiştir. Türkiye'de de bu yönde kripto para kullanıcıları için hizmet veren borsalar bulunmaktadır. Bu borsalardan bazıları ise BtcTurk, Koinim.com, Koineks, Coinbase dir (Özden, 2019: 30). Türkiye'de önde gelen bu borsalar ise Tablo 14'de dünya üzerindeki borsaların açıklandığı gibi açıklanarak bu konuya aydınlık kazandırılmaya çalışılmıştır.

Tablo 14: Türkiye'de Önde Gelen Kripto Para Borsaları

Kripto Para Borsası	Borsanın Özelliği
Sistemkoin	2018 yılı içerisinde Balıkesir Bandırma'da açılmıştır. Bitcoin ve Altcoin'ler açısından en büyük işlem hacmine sahip tezgah üstü piyasa olarak bilinmektedir. Türkiye'de ilk sırada yer alan kripto para borsasıdır. Borsada işlem yapabilmek için ad, soyad, telefon numarası, e-mail adresi gerekli olup aynı zamanda bir şifre belirlenerek üye olunmaktadır. Başkalarını referans gösterdikten sonra ise referans işlem gerçekleştirdiğinde %20 oranında bir bonus kazanılmaktadır. Coin yatırımlarının %98 oranı soğuk cüzdanlarda saklanılmaktadr. Yatırma ve çekme işlemi yaklaşık 15 dakika sürerken en fazla banka ile anlaşmalı olarak çalışan kripto para borsası olma özelliğine de sahiptir.
Vebitcoin	Muğla merkezli bir borsadır. TL'nin dışında Euro ve ABD Doları ile de işlem yapılmasına izin vermektedir. Türkiye'nin en büyük ikinci kripto para borsası olma özelliğine sahiptir. Üyelik işlemin gerçekleştirilmesi yönünden Sistemkoin'e benzemektedir.
Ovis	KKTC merkezli olup bünyesinde 25'ten fazla Altcoin bulundurmaktadır. Yatırımcılara ise yeni oyuncu ve deneyimli oyuncu olmak üzere 2 farklı yönetim ekranı sunmaktadır. En önemli özelliği kendi kripto para teknolojisine ve alt yapısına sahip olmasıdır. İki adımlı doğrulama (2FA), IP kısıtlama, yazılım analizi ve şifreleme ile güvenlik sağlanmaktadır. Referans durumunda ise %25 oranında komisyon kazanılabilmektedir.

BTCTürk	Türkiye'nin ilk ve en popüler borsası olup dünyadaki en güvenilir ilk 10 kripto para borsaları arasında 7. Sırada yer almaktadır Bitcoin üretimi için herhangi bir hizmet sunmamakla birlikte TL üzerinden işlem yapmak isteyen kullanıcılara yerel bir seçenek olarak varlığını sürdürmektedir. 2013 yılında kurulmuş olup TL tabanlıdır ve 2018 yılı itibariyle 55 bin aktif kullanıcıya ulaşmıştır. Kripto paraların alımı ve satımı bilgisayarların yanı sıra mobil aygıtlar aracılığıyla da yapılabilmektedir. Soğuk depolama yöntemi sayesinde güvenlik sağlanmaktadır. 100.000 TL' e kadar gerçekleştirilen işlemlerde piyasa yapıcısı için % 0,20; piyasa alıcısı için % 0.30 komisyon alınmaktadır.
Paribu	Paribu bünyesinde Bitcoin, Ethereum, Ripple, Tron, Holo, Litecoin, Bitcoin Cash, Stellar, Dogecoin, Cardano, Neo Tether, Eos gibi on üç kripto para işlem görmektedir. Bir banka dan Paribu hesabına en az 500 TL yatırıldıktan sonra Bitcoin alım işlemleri gerçekleştirilmektedir. Para transfer işlemi EFT aracılığıyla yapılabilmektedir. Minimum çekim miktarı ise 10 TL'dir. Girişte çift aşamalı doğrulama yöntemi kullanılarak güvenlik sağlanmaktadır. Aynı zamanda soğuk depolama yöntemi ile bu güvenlik seviyesi üst düzeye çıkarılmaktadır. 50.000 TL' ye kadar gerçekleştirilen işlemlerde piyasa yapıcısı için % 0,3; piyasa alıcıları için % 0,4 oranında komiston alınmaktadır. Ayrıca bu borsadan TL çekilirken 3 TL; Bitcoin çekilirken 0.0005 BTC ücret alınmaktadır.
Koineks	Soğuk depolama ve çift faktörlü kimlik tanıma yöntemi ile güvenlik sağlanmaktadır. Üyelik için ücret gerekmemekle birlikte işlem yapılabilmesi için hesaba TL yüklenilmesi gerekmektedir. TL yatırma işlemleri hafta içi 09.00 ve 18.00 saatleri aracında onaylanmaktadır. 250.000 TL' ye kadar gerçekleştirilen işlemlerde piyasa yapıcısı için %0,2; piyasa alıcısı için % 0, 3 oranında komisyon alınmaktadır. Herhangi bir bankadan Koineks'e para yatırırken ücret alınmamasına karşın Koineks'ten TL çekilirken 3 TL ücret alınmaktadır. Aynı zamanda kural dışı banka transferi gerçekleştirildiğinde iade kesintisi olarak 4 TL ücret alınmaktadır.

Bithesap	Hehangi birini referans etmeleri durumnda 10 TL değerinde hediye vermektedirler. 30 günlük işlem hacmi 50.000 TL olan kullanıcı 1.000 TL değerinde Bitcoin aldığı zaman 2 TL komisyon ücreti ödemektedir. Kullanıcıların Bithesap'ta bulunan hesaplarına para yatırdıkları zaman ücret alınmamakta ancak para çekerken 5 TL ücret alınmaktadır. Hatalı banka tranferi için 10 TL ücret alınmaktadır. Onaylanmamış bir hesap için ise günlük 500 TL ve aylık 5.000 TL; onaylanmış hesaplarda günlük 100.000 TL ve aylık 500.000 TL sınır bulunmaktadır.
Koinim	TL, Bitcoin, Litecoin ve Bitcoin Cash alım-satım işlemleri yapanlara hizmet vermektedir. Dolayısıyla BTC-TL değişimi yapılabilmektedir. Ayrıca kullanıcılarına sunduklarıhizmetler ile alıcı ve satıcıyı buluşturup bu aracılık hizmetleri karşılığında komisyon elde etmektedirler. 30.000 TL'ye kadar olan işlemlerde % 0, 4; 30.000 TL üzeri işlemlerde % 0, 3 komisyon alınmaktadır. Koinim hesabına para yatırırken ücret alınmazken hesaptan TL çekildiğinde 3 TL; Bitcoin çekildiğinde 0.001 BTC; Litecoin çekildiğinde 0.015 LTC ve son olarak Bitcoin Cash çekildiğinde 0,0005 BTCash ücret alınmaktadır.

Kaynak: (Metin ve Alptekin, 2018: 179-189; Aba Şenbayram, 2019: 88; Ceylan, 2019: 45; Karaçalı, 2019: 43).

Yukarı verilen Tablo 13 ve Tablo 14 üzerinden de görüleceği üzere dünya üzerinde kripto paralara olan ilginin sürekli artmasıyla birlikte kripto para borsalarının sayısında sürekli artış yaşanmıştır. Eğer kripto paralara olan ilgide bir azalma yaşanmazsa bu borsaların sayısında da sürekli artışlar yaşanmaya devam edecektir.

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA VE DÖVİZ KURU İLİŞKİSİ: UYGULAMALI ZAMAN SERİSİ ANALİZİ

Çalışmanın bu bölümüne kadar kripto paralara ve işleyişlerine yönelik teorik altyapı açıklanmıştır. Bu bölümde ise bu konuda daha önce yapılmış teorik ve uygulamaya yönelik literatür ayrı ayrı incelenmiş ve bu çalışmalar aracılığıyla konuyla ilgili genel bir bilgi elde edinilmeye çalışılmıştır. Bu yapılan çalışmalardan hareketle literatürde ihtiyaç duyulan ve aydınlatılması gereken kısım tespit edilmiş ve bu doğrultuda çalışmanın bu bölümünde öncelikli olarak kripto para ve döviz kuru arasındaki ilişkinin ekonometrik olarak analiz edilmesi amaçlanmıştır. Bu doğrultuda kripto paranın temsilcisi olan Bitcoin ile majör para birimlerinin çapraz kur değerlerinden yararlanılarak amaca ulaşılmaya çalışılmıştır. Yapılan analiz sonuçları ve bu yönde uygulanan analizlerin teorik altyapısı çalışmanın bu bölümünde açıklanmıştır.

3. 1. LİTERATÜR ARAŞTIRMASI

Bitcoin'in ortaya çıktığı günden bugüne kadar kripto paraların yeni bir yatırım veya kâr aracı olabileceği düşüncesiyle bu paralar birçok girişimcinin ilgisini çekmeyi başarmıştır. Zaman geçtikçe de ilgi daha da artış göstermiş ve bilim dünyasında kripto paralar üzerine yapılan çalışmalarda artış gözlenmiştir. Çalışmanın bu bölümünde kripto paralar üzerinde yapılmış ve literatüre önemli katkılar sağlamış çeşitli akademik çalışmalara yer verilmiştir. Bu bağlamda öncelikli olarak teoriye yönelik çalışmalara daha sonra uygulamaya yönelik analiz çalışmalarına ayrıntılı bir şekilde yer verilmiştir.

3. 1. 1. Teoriye Yönelik Kripto Para Literatürü

Catalini ve Gans (2018), Bitcoin'in şifreleme sistemine dayanıp eşler arası elektronik nakit sistemi olarak 2008 yılının Ekim ayında Satoshi Nakamato tarafından ortaya çıkarıldığını söylemişlerdir. Mantıklı bir şekilde şifreleme ve oyun teorisinin bir araya getirilmesinin, blockchain teknolojisi yoluyla, kripto para birimlerindeki işlemlerin ucuz bir şekilde doğrulanmasına yardımcı olacağı ifade edilmiştir. Diğer yandan çalışmada öncelikli olarak blockchain teknolojisinden etkilenen doğrulama ve ağ oluşturma maliyetlerine odaklanılmıştır. Bu doğrultuda blockchain teknolojisinin döviz ağlarının işletme maliyetlerini yani ağ oluşturma maliyetlerini büyük ölçüde düşürdüğünü belirtilmiştir.

Fatima ve Tiwari (2018), Bitcoin'in devlet ya da bankalar gibi izlenmesi gereken merkezi bir otorite olmadan, tamamen eşler arası bir ağa dayandığı ve dünyanın ilk merkezi olmayan dijital para birimi olarak kabul edildiği belirtilmiştir. Aynı zamanda işlemlerin, ağ düğümleri tarafından kriptografi kullanılarak doğrulandığı ve halka açık bir deftere kaydedildiğini söylemişlerdir. Çalışmada bu çerçevede blockchain teknolojisine odaklanılmıştır. Blockchain'i tanımlamak için işlemlerin doğruluğunu garanti ederken, deftere kaydedilen verilerin herhangi bir şekilde değiştirilmesini önlemek amacıyla kriptografik karma işlemlerden yaralanan, eşler arası bir ağda dağıtılmış defter ifadesini kullanmışlardır. Aynı zamanda bu teknolojinin merkezi bir otorite tarafından kontrol edilmeyip blokların çoğaltılmasına dayandığını ve her bloğun bir önceki bloğun karmasını içerdiğini söylemişlerdir. Dolayısıyla işlemlerin bir kere kaydedildiğinden dolayı bir bloktaki verilerin, sonraki tüm blokları değiştirmeden geriye dönük olarak değiştirilemeyeceğine vurgu yapılmıştır.

Salviotti, De Rossi ve Abbatemarco (2018), kripto para birimlerinin şifreleme teknolojisi kullanılarak ortaya çıkarılan elektronik bir para birimi olduğu ve bu şifreleme para piyasasında en yaygın kullanım görenlerinin Bitcoin ve Ethereum olduğu dile getirilmiştir. Yazarlar bu para birimlerinin blockchain olarak isimlendirilen Blokzincir teknolojilerinin özgün ve ilk örneklerinden olduğunu ifade etmişlerdir. Bu açıdan da çalışmalarında özellikle blockchain teknolojisine ağırlık verip bu yönde çalışmalarını şekillendirmişlerdir. Çalışma kapsamında aynı zamanda kripto para birimlerinin herkes tarafından programlanabilen ve üçüncü kişilere gerek

kalmadan taraflar arasında finansal ağ kurmayı kolaylaştıran dolayısıyla bankacılık sistemine olan bağlılığı azaltan bir algoritma olduğu da belirtilmiştir. Şifreli paranın bu olumlu yönlerinin yanı sıra dijital güvenlik, piyasa düzenlemeleri ve spekülatif saldırı gibi bazı zayıf yönlerinin olduğuna da dikkat çekilmiştir.

Söderberg (2018-a), esas olarak İsveç'te nakit kullanımındaki düşüşün bir sonucu olarak e-krona adı verilen yeni bir dijital para çıkma olasılığından hareket edilerek bir paranın ne olduğu ve e-krona'nın ne tür bir para olacağı tartışılmıştır. Çalışmada ilk olarak paranın tam olarak ne olduğu yönünden net bir tanımı yapılamadığı ve teknolojik gelişmeler ile birlikte paranın kullanımında değişiklikler meydana geldiği ifade edilmiştir. Bu değişikler sonucunda kripto para birimlerinin gündeme gelerek bu paraların, kriptografik hesaplamalar ile kullanıcılara aktarılan dijital para birimi olduğu ve merkezileştirilemediği belirtilmiştir. Diğer yandan kripto paraların ilk olarak 2009 yılında Bitcoin ile ortaya çıkıp Bitcoin en büyük kripto para birimi olduğu ancak Ethereum gibi diğer kripto para birimlerinin de sürekli olarak pazar paylarını artırdığı vurgulanmıştır. Bu gelişmelere rağmen kripto paraların, paranın ne olduğuna dair temel görüşlerden herhangi birine göre, para olarak sınıflandırılamayacağı da ifade edilmiştir. Çalışmada para piyasasındaki bu gelişmelerle birlikte ise İsveç Merkez Bankası tarafından verilen bir dijital para sorununun ortaya çıktığı ifade edilip e-krona odaklanılmıştır. Bu doğrultuda e-krona'nın bir devlet otoritesi tarafından verildiği ve hiçbir şekilde bağımsız bir para birimi olmayacağı söylenmiştir. Bu bağlamda e-krona'nın, kripto paralardan farklı olarak bir güvene sahip olduğu ve değerinin kripto para birimlerinden farklı şekilde değişeceği belirtilmiştir.

Söderberg (2018-b), çalışmasında kripto varlıkların niteliği, gelişimi ve para olarak kabul edilip edilemeceğini tartışmıştır. Yazara göre bir kişi kripto paralara ödeme ve bir yatırım aracı olmak üzere iki ana sebepten dolayı sahip olmaktadır. İkinci durumdaki kişiler fiyatın yükseleceği umudunu korumak için kripto varlıkları satın alırken gerçek bir ödeme aracı olarak kullanıldığına dair kesin bir fikir olmadığı da çalışma kapsamında ileri sürülmüştür. Aynı zamanda birçok farklı kripto varlıkların olduğu dolayısıyla genel bir bakışa sahip olmanın mümkün olmamakla birlikte, kripto paraların yüksek volatiliteye sahip olduğu belirtilmiştir. Bunun etkisiyle sürekli fiyat düşüşleri riski taşıdığı ve bu durumun bireyler için büyük kayıplara yol açabileceği ve bireylerin bu yönde korunamayacağı yönünden uyarı

yapılmıştır. Kripto varlıkların para olarak değerlendirilip değerlendirilemeyeceği yönünden ise, bu varlıkların hiçbir vericiye sahip olmaması, henüz etkin ödeme araçları sağlama kabiliyetinin bulunmaması ve sabit bir değerin korunmasında zorluk çekmesi gerekçesiyle para olarak sınıflandırılamayacağı görüşü savunulmuştur.

Thakur ve Banik (2018), kripto parayı, güvenlik amacıyla şifreleme sistemi kullanılan dijital ve sanal bir para birimi olarak tanımlamışlar ve bu güvenlik özelliği nedeniyle kripto paraların sahte olmasının zor olduğunu ifade etmişlerdir. Çalışmada en yaygın kripto para birimlerinden olan Bitcoin üzerinde de durulmuş ve Bitcoin'in elektronik alımlar ve transferler için kullanılırken aynı zamanda çoğu yerde geçerli olduğunu da dile getirmişlerdir. Bu kripto para birimlerinin avantajının, yapılan işlemin günlük olarak hemen dijital ortama kaydedilmesi olduğunu söylemişlerdir. Thakur ve Banik kripto paranın, devlet müdahaleleri ile manipülasyonlara karşı güçlü olup herhangi bir merkezi otoriteye bağlı olmadan işlem gördüğünü ve bunun kripto parayı diğer para birimlerinden ayıran en önemli özelliklerinden biri olduğunu belirtmişlerdir.

Devries (2016), dijital takas işlemlerini kolaylaştırmak amacıyla şifreli bir ağ sistemi ile işlem gören kripto paraların, son birkaç yıl içerisinde gelişmeye başlayan bir teknoloji olduğunu dile getirmiştir. Çalışmada kripto para birimlerinin gelecekte geleneksel para birimlerinin yerini alabileceği yönünden bir kesinlik olmasa bile, internet bağlantılı küresel pazarların birbirleriyle olan etkileşim biçimlerini değiştirerek, küresel pazarlardaki ulusal para birimlerinden ve döviz kurlarından kaynaklanan engelleri ortadan kaldırabileceğinin üzerinde durulmuştur. Bu açıdan kripto para birimlerinin, serbest akışlı bir işlem sistemi oluşturarak ticaret piyasalarında bir devrim yaratabileceğine dikkat çekilmiştir. Bu şifreli para birimlerinin aynı zamanda mikro işlemleri yapabilmesinden dolayı, geleneksel para birimlerinin çözemeyeceği ve daha derin bir ekonomik analiz yapılması gereken durumlarda kullanılabileceği dolayısıyla ekonomik sorunların çözümünde de yardımcı olabileceği ifade edilmiştir.

Harwick (2016), çalışmasında Altın'ın tarihsel geçmişi çerçevesinde, kripto para birimlerinin gelecekte karşılaşabileceği teknik, yasal ve ekonomik engelleri araştırırken bu para birimlerindeki finansal aracılığın kendine özgü sorunlarına odaklanmıştır. Bu doğrultuda kripto para birimlerinin ve özellikle Bitcoin'in gelecekteki ilerlemesinin sadece istikrarlı bir alım gücünün elde edilmesine bağlı

olmadığını ifade etmiştir. Çalışmada bu noktaya gerekçe olarak, finansal aracı piyasası dışındaki bir para birimi için talep esnekliği sağlansa bile bunun tek başına ekonomik büyüme ve verimlilik için yeterli olmayacağı aynı zamanda böyle bir piyasa ortamının kripto para birimlerinin yasal olarak desteklenen para birimlerine bağlı kalmasına neden olacağı gösterilmiştir.

Luther (2016), mevcut para birimlerinin, Bitcoin'in benimsenmesinin önündeki en büyük engel olduğu ifade edilmiştir. Çünkü Bitcoin'in kullanma kararının alınması aynı zamanda yerleşik bir para birimini bırakma kararını göstermekte ve bu da maliyetlerde değişiklik yapılacağına işaret edip otomatik vezne makinelerinin yeniden biçimlendirilmesi, işlem kayıtlarının güncellenmesi ve hatta hesap birimi olarak değerlendirilip yeni hesaplama sistemini öğrenme anlamına gelmektedir. Diğer yandan mevcut para birimlerinin hükümetler tarafından desteklenirken Bitcoin'in desteğe tâbi olmanın aksine bazı hükümetler tarafından yasaklanmaya çalışılması da bu kripto para açısından bir dezavantaj olarak nitelendirilmektedir. Bu amaçla Bitcoin'in mevcut bir parayı değiştirebilmek için anahtarlama maliyetlerini garanti altına alması ve anahtarlama maliyetlerinden arındırılmış mevcut bir paradan daha iyi olması gerekmektedir. Bitcoin aynı zamanda kendisinden sonra gelen diğer kripto para birimleriyle de karşı karşıya kalmaktadır. Ancak bu noktada Bitcoin gibi diğer kripto paralarda mevcut paralar ile rekabet etmek zorunda kalıp bu da Bitcoin'in için bir avantaj teşkil etmektedir.

Nair ve Cachanosky (2016), piyasa sürecinde mevcut bir para biriminden yeni bir para birimine kendiliğinden geçiş için var olan mekanizma incelenmektedir. Bu doğrultuda Bitcoin, dünyanın ilk başarılı şifreli para birimi olarak kabul edilip Merkez Bankası gibi tekel para biriminin ihracına duyulan ihtiyacı ortadan kaldırırken aynı zamanda sabit bir para arzı sağlamaktadır. Bunun yanı sıra doların ve diğer yerleşik para birimlerinin güçlü varlığı nedeniyle önemli engeller ile karşı karşıya kalmaktadır. Çünkü böyle bir ortamda piyasaya yeni giren bir para birimi olan Bitcoin'in daha yüksek bir arama maliyetleriyle karşı karşıya kalması beklenmektedir. Bu noktada girişimcilerin uyanıklığı, en azından Bitcoin'in benimsenmesi ve özellikle potansiyel bir kendiliğinden değişime izin veren mekanizmaların uygulamaya girmesi için kredi niteliği taşımaktadır.

Rabah (2016), dijital paranın, fiziksel para birimlerine benzer özellikler sergileyip anlık işlemlere ve sınırsız mülkiyet devrine izin verdiğini ancak geleneksel

paralardan farklı olarak internet tabanlı bir döviz aracı olduğunu belirtmiştir. Rabah çalışmasında kriptografi olarak isimlendirilen şifreleme sistemini kullanarak dijital imzaların arkasındaki matematik algoritmayı ve bunun Bitcoin gibi kripto para birimlerinde ve madencilikte nasıl uygulandığını sunmuştur. Bu doğrultuda kripto paraların bağlı bilgisayar ağları tarafından paylaşılıp blokzincir olarak adlandırılan defterlere kayıtlarının tutulduğunu söylemiştir. Çalışmada blokzincir çerçevesinde oluşturulan özel anahtarlar ile bu kripto paraların güvenliğinin sağlandığı dile getirilmiştir. Bu güvenliğin ise özel anahtarların imzası ile açık anahtarların eşleştiği bir komut dosyasının, Bitcoin adresine bağlı olması suretiyle işlem yapmaya izin vermesiyle sağlandığı belirtilmiştir.

Scott (2016), kripto para birimi, işbirliğine dayalı açık kaynak ilkelerine ve karşılıklı dayanışma gerektiren eşler arası ağlara dayanmaktadır. Kripto para içerisinde önemli bir yere sahip olan Bitcoin sisteminin normal bankacılık ödeme sisteminden temelde iki önemli farkı bulunmaktadır. Bunlardan ilki insanlar arasındaki ödemeleri kaydetmek için kullanılan veri tabanının, normal bankacılık sisteminde özel olarak tutulurken Bitcoin sisteminde halka açık olmasıdır. İkinci en önemli fark ise Bitcoin sisteminde, kendi özel yazılım sistemini işleten bankalar yerine merkezi olmayan bir insan ağına dayanmasıdır. Bu nedenle Bitcoin sistemi, insanların kendi aralarında dijital belirteçlerin işlemlerini kaydetmek için kullanabileceleri, blokzincir olarak adlandırılan, dağıtılmış ve halka açık bir deftere veya veri tabanına sahip olup bu şekilde belirteçlerin puanını halka açık ve şeffaf bir şekilde tutabilmektedir.

Gipp, Meuschke ve Gernandt (2015), güvenilir zaman damgasının belirli bilgilerin belirli bir zamanda var olduğunu kanıtlamak için yapılan bir işlem olduğunu ifade ederken bu merkezi olmayan güvenilir zaman damgası kavramını ve veri bütünlüğünü doğrulamak için kripto parayı kullanmışlardır. Buna göre kripto para işlemlerinde kullanılan zaman damgasında işlemler bu şifreli para biriminin blokzincirine yani tüm işlemlerin kriptografik olarak doğrulanmış olduğu deftere kaydedilmektedir. Bir bankanın defterinin aksine blokzincir, tek bir varlığa bağlı değilken kripto para birimi ağına katılan ve herkes tarafından halka açık olan tüm bilgiler, işlem düğümleri tarafından yedekli olarak korunmaktadır.

Brill ve Keene (2014), son yıllarda kripto para birimi olarak bilinen yeni bir para türünün kullanıldığını ve bu para birimlerinden en yaygınının Bitcoin olduğunu

dile getirmişlerdir. Çalışmada bu kripto para birimlerinin herhangi bir ülkede hükümet tarafından ihraç edilmediği ve hükümet desteğine tâbi olmadığı da belirtilmiştir. Buna rağmen sanal para birimlerinin hem küresel fon transferinde önemli bir faktör haline gelmesi gibi küresellik hem de anonimlik özelliğinden dolayı kabul gördüğüne dikkat çekilmiştir. Brill ve Keene bu para birimlerinde devlet desteği olmamasına rağmen, dünyanın her tarafında kişiden kişiye kolayca aktarılabilmesi, her türlü alım-satım işlemlerinde kullanılabilmesi ve fonlarının ulusal sınırlar boyunca hızlı, sessiz ve düşük maliyetle hareket edebilmesinden dolayı cazip hale geldiğini söylemişlerdir. Çalışmada tüm bu olumlu yönlerinden dolayı kripto para birimlerinin siber suçlular, uyuşturucu satıcıları, kara para aklayıcılar ve küresel terör fonu ile ilgili olanlar içinde cazip hale gelmesi gibi olumsuz yönlerinin de olduğuna dikkat çekilmiştir. Bu açıdan gerekli önlemlerin alınması gerektiğine aksi halde bu para birimlerinin kötüye kullanılabileceğine de vurgu yapılmıştır.

Luther ve White (2014), özel bir şifreli para birimi olan Bitcoin'in sürekli olarak yayılmasının ekonomistlerin ilgisini çektiğini bundan dolayı da piyasada nasıl oynaklık ve gelişme göstereceğinin merak edilip incelendiğini söylemişlerdir. Bu doğrultuda iki farklı görüş olup bir tarafın Bitcoin'in kendi kendini besleyen bir balon olduğu düşüncesine sahipken diğer tarafın eşler arası şifreli ödeme teknolojisinde lider olarak büyük bir büyüme öngördüğü düşüncesine sahip olduğu belirtilmiştir. Luther ve White, Bitcoin'in çoğunlukla spekülatif bir araç olarak tutulup Bitcoin'in değerindeki belirsizlikten dolayı mal ve hizmetlerin bedelinin ödenmesinde çok fazla kullanılmadığını belirtmişlerdir. Çalışmada Bitcoin'in değerindeki bu belirsizliğin nedenini açıklamaya çalışmışlar ve en temel nedeninin yükselen talep karşısında Bitcoin arzının esneklik göstermemesi olduğuna dikkat çekmişlerdir.

Yermack (2013), Bitcoin'in para birimi olarak kabul edilip edilmemesi gerektiğini incelemiş ve tamamen para birimi gibi hareket sergilemediğini ileri sürmüştür. Ancak yazara göre Bitcoin, paranın en önemli özelliklerinden biri olan değişim aracı olma özelliğini gösterdiğinden dolayı para birimi olarak değerlendirilebilmektedir. Diğer yandan Bitcoin'in volatilitesinin çok yüksek olması ve arbitraj olasılığı olmadan farklı borsalarda farklı fiyatlarda işlem görmesinden dolayı, paranın diğer özelliklerinden olan, hesap birimi ve değer saklama aracı olarak kullanılmada yetersiz kaldığı dile getirilmiştir. Bu doğrultuda Bitcoin'in tam anlamıyla para birimi olarak değerlendirilebilmesi için günlük değerinde istikrarın

sağlanması gerektiği söylenip böylelikle Bitcoin'in bir değer deposu ve ticari piyasalarda güvenilir bir hesap birimi olarak hizmet verebileceği belirtilmiştir.

3. 1. 2. Analize Yönelik Kripto Para Literatürü

Bhosale ve Mavale (2018), kripto para birimini işlemleri güvence altına almak ve varlıkların transferini doğrulamak için şifreleme kullanan aynı zamanda bir değişim aracı olarak çalışmak üzere tasarlanmış dijital bir varlık şeklinde tanımlamışlardır. Çalışmada kripto para birimleri içerisinde Bitcoin'in özellikle son zamanlarda daha da dikkat çekmeye başladığı ve bu durumun alternatif kripto para birimlerinin ortaya çıkmasına neden olduğu dolayısıyla da bunların karşılaştırılması gerektiği düşüncesinden hareket edilmiştir. Bu doğrultuda kripto para birimlerinin en yaygın türlerinden olan Bitcoin, Ethereum ve Litecoin'in son zamanlardaki oynaklıkları ve istikrarları karşılaştırılarak sergilemiş oldukları eğilimler anlaşılmaya çalışılmıştır. Çalışmada analizi gerçekleştirmek amacıyla kripto paranın oynaklığının çok yüksek olduğu Aralık 2017 ve Ocak 2018 verileri karşılaştırılmıştır. Bunun sonucunda Bitcoin'in volatilitesi en yüksek kripto para birimi olduğu ve beş yıl içinde kullanım oranlarının daha fazla büyüme yaşayabileceği anlaşılırken aynı zamanda Ethereum ve Litecoin'in piyasaya yeni girilen paralar ile karşılaştırmalı olarak artan bir eğilim gösterdiği ancak Litecoin'in Ethereum'dan daha az çeşitlilik gösterip yeni yatırım seçeneği olarak Litecoin'in tercih edilebileceği sonucuna ulaşılmıştır.

Çütçü ve Kılıç (2018), dijital paranın, uluslararası ticarette önemli bir paya sahip olduğundan ve diğer para birimlerinde olduğu gibi hem tasarruf hem de yatırım aracı olma özelliği gösterdiğinden dolayı öneminin giderek arttığını belirtmişlerdir. Dijital paranın kullanım oranlarının sürekli artıyor olmasına bağlı olarak dijital para borsalarının da oluşmaya başladığına dikkat çekmişlerdir. Bu çerçevede kripto paranın kullanımının günümüzde giderek arttığını söyleyip buna kanıt olarak da Bitcoin'in işlem hacmini örnek olarak göstermişler ve çalışmalarını bu yönde şekillendirmişlerdir. Çalışmada Bitcoin ile döviz kurları arasındaki yapısal kırılmalar incelenerek uzun ve kısa dönemli ilişkilerini analiz etmeye çalışmışlardır. Analizi gerçekleştirebilmek amacıyla 24 Kasım 2013 ve 4 Mart 2018 tarihleri arasındaki haftalık verilerden yararlanmışlardır. Çalışmada yapılan maki eşbütünleşme testi sonucunda Bitcoin ile döviz kuru arasında hem orta hem de uzun dönemli bir ilişkinin

olduğunu ve Bitcoin fiyatlarının döviz kurundaki dalgalanmalardan ciddi derecede etkilendiğini ortaya koymuşlardır.

Kanat ve Öget (2018), günümüzde kripto paranın önemi giderek arttığından dolayı Bitcoin fiyatlarını ele alarak analiz yapmışlardır. Çalışmada, Bitcoin fiyatlarından hareketle, G-7 ülkeleri ile Türkiye arasındaki hem uzun hem de kısa dönemli nedensellik ilişkisi, ekonometrik analiz çerçevesinde açıklanmaya çalışılmıştır. Analizi gerçekleştirmek için gerekli verileri bulmaya çalışırken, Bitcoin'in 2013 yılında dalgalanmalar göstermeye başladığı düşüncesinden hareketle, 1 Ocak 2013 tarihinden başlayarak 1 Ocak 2018 tarihine kadarki değerlerden yararlanmışlardır. Elde ettikleri veriler doğrultusunda yaptıkları eşbütünleşme testi sonucunda ise Bitcoin ile borsalar arasında uzun dönemli bir ilişkinin olduğu ancak bu ilişkinin belli bir düzen izlemediği ve Bitcoin'in borsalardan bağımsız hareket ettiği sonucuna ulaşmışlardır.

Lee, Guo ve Wang (2018), Bitcoin'nin Satoshi Nakamoto tarafından 2008 yılında icat edildiğini ve bununla birlikte Altcoin olarak bilinen birçok yeni kripto para biriminin ortaya çıktığını söylemişlerdir. Bu kripto para birimlerinin hepsinde benzer kriptografi teknolojisinin kullanılmasına karşın farklı algoritmik tasarımların kullanıldığı da dile getirilmiştir. Çalışmada kripto para biriminin dijital paraların bir alt türü olmasına rağmen giderek daha da önemli bir dijital para birimi haline geldiğine ve diğer dijital para birimlerinden çok daha farklı özellikler sergilediğine dikkat çekilmiştir. Bu farklılıklar arasında ise kripto paranın üçüncü kişilere gerek duymadan daha güvenli ve daha hızlı işlem yapmaya izin vermesi gösterilmiştir. Çalışmada analiz kapsamında ise geleneksel varlık sınıfları ile kriptografik para endeksi (CRIX) arasındaki ilişki korelasyon katsayıları doğrultusunda incelenmiş ve aralarında çok düşük bir korelasyon olduğu, çoğu kripto para birimlerinin günlük getirilerinin geleneksel yatırımlarınkinden daha yüksek olduğu sonucuna ulaşılmıştır. Bu doğrultuda CRIX ve kripto para birimlerinin portföy risklerini çeşitlendirmeye yardımcı olacağı yorumunda bulunmuşlardır.

Sovbetov (2018), çalışmada 2010-2018 dönemi arasındaki haftalık veriler kullanılarak, en yaygın beş kripto para biriminden olan Bitcoin, Ethereum, Dash, Litecoin ve Monero'nun fiyatlarını etkileyen faktörler incelenmiştir. Elde edilen veriler doğrultusunda değişkenler arasındaki ilişkiyi incelemek amacıyla ARDL analizi yapılmıştır. Yapılan analiz sonucunda, kripto para piyasındaki oynaklıkların ve

piyasanın ticaret hacminin, ele alınan bu beş kripto para birimi üzerinde, hem uzun hem de kısa dönemde önemli bir etkisi olduğu açıkça belirtilmiştir. ARDL analiziyle birlikte, bu beş kripto para birimi içerisinden, Bitcoin ve Ethereum'un uzun vadede piyasaya daha yüksek yanıt verdiği ancak bu iki kripto para biriminin, kısa dönem katsayılarının uzun dönem katsayılarına göre daha yüksek olduğundan dolayı, bu yanıtlarının kısa dönemde daha hassas olduğu sonucuna ulaşılmıştır.

Chu, Chan, Nadarajah ve Osterrieder (2017), kripto parayı, değişim aracı olmak üzere tasarlanmış ve işlemleri güvence altına almak amacıyla şifreleme sisteminin kullanıldığı dijital bir varlık olarak tanımlamışlardır. Çalışmada kripto para birimlerinin geleneksel para birimlerine kıyasla oldukça değişken bir yapıda olduğu belirtilmiş ve kripto paranın oynaklığını analiz etmek amacıyla GARCH modelinden yararlanılmıştır. Analizi gerçekleştirebilmek amacıyla Bitcoin, Dash, Dogecoin, Litecoin, Maidsafecoin, Monero ve Ripple gibi en popüler 7 kripto para birimlerinin günlük küresel fiyat endekslerinden yararlanılmıştır. Yaptıkları analiz sonucunda ise kripto para birimlerinin özellikle günlük fiyatlarında aşırı oynaklık gösterdiğini ortaya koymuşlardır. Bunun ise özellikle teknoloji pazarlarına yatırım yapıp risk üstlenen yatırımcılar için uygun olduğunu dile getirmişlerdir.

Dirican ve Canöz (2017), çalışmalarında ilk olarak elektronik para ile kripto para arasındaki farkı açıklamaya çalışmışlardır. Bu doğrultuda en önemli farkın elektronik parada; MB, bankalar ve uygun koşulları sağlamak koşuluyla tüzel kişiliklere sahip firmaların ihracatçı olabileceğini ancak kripto parada; ihracatçının bir tüzel kişinin olmak zorunda olmadığı, merkezi kurumlardan bağımsız kişilerin ya da kurumlarında ihracatçı olabileceğini belirtmişlerdir. Dirican ve Canöz çalışmalarında en çok dikkat çeken kripto para biriminden olan Bitcoin üzerinde durmuşlar ve Bitcoin'in yatırım ve yatırım kararlarına olan etkilerini ARDL yöntemiyle analiz etmişlerdir. Analizi gerçekleştirebilmek amacıyla 24 Mayıs 2013 ile 5 Kasım 2015 dönemleri arasındaki haftalık Bitcoin fiyatlarından ve bazı hisse senetleri piyasa endekslerinden yararlanmışlardır. Bitcoin fiyatlarına ait verilere ulaşmak için Bitcoin'in en çok işlem gördüğü 5 piyasa verilerinden yaralanmışlar ve bunlar içerisinden en büyük paya sahip borsanın Bitfinex olduğu sonucuna ulaşmışlardır. Analiz sonucunda ise Bitcoin fiyatları ile ele alınan hisse senetleri endeksleri arasında kısa dönemli bir ilişkinin olmadığı ancak uzun dönemli bir ilişkinin kendini gösterdiğini ifade etmişlerdir.

Dulupçu, Yiyit ve Genç (2017), çalışmalarında Bitcoin'in fiyatı ile popülaritesi arasındaki ilişkiyi incelemişlerdir. Analiz için gerekli verilerin rakamsal olarak yüksek olmasından dolayı varyans salınımını engellemek amacıyla verilerin logaritması alınmış ve bunun sonucunda değişkenlerin hepsi seviyede durağan hale getirilmiştir. Değişkenlerin hepsi seviyede durağan olduğu için değişkenler arasındaki ilişkiyi analiz etmek amacıyla, VAR analizi uygulayıp, varyans ayrıştırması ve Granger nedensellik testi yapılmıştır. Çalışmada yapılan White testi sonucunda hata terimleri varyansının sabit olduğu sonucu kabul edilmiş ve varyans ayrıştırması sonucunda Bitcoin'in piyasadaki miktarının fiyattaki değişimi açıklamada yetersiz kaldığını ortaya koymuşlardır. Bu doğrultuda Bitcoin'in dolaşımdaki miktarının dışsal bir değişken olduğu ve diğer değişkenlere bağlı olmadığı yorumunu yapmışlardır. Çalışmada son olarak Granger nedensellik testi yapılıp bunun sonucunda Bitcoin'in fiyatı ile popülaritesi arasında tek yönlü bir ilişkinin olduğu açıklanmıştır. Sonuç olarak çalışmada Bitcoin'e yönelik ilgi ve talep arttıkça Bitcoin'in fiyatlarının yükseldiği ortaya çıkarılmıştır.

Elbahrawy vd. (2017), son zamanlarda finansal dünya içerisinde, kripto para birimlerine olan ilginin sürekli olarak artmasına rağmen, çalışmalarda sadece birkaç tane kripto para birimine odaklanılıp, bu konuda tüm sistemi içerisine alan kapsamlı bir çalışmanın eksikliğinden hareket ederek çalışmalarını şekillendirmişler. Bu açıdan çalışmada farklı olarak kripto para birimi piyasalarının tam analizi yapılmış ve farklı kripto para birimlerinin pazar paylarına odaklanılmıştır. Bu amaçla 157 döviz piyasası platformundan, 28 Nisan 2013 ile 13 Mayıs 2017 dönemindeki haftalık verileri toplayarak, aktif kripto para birimlerinin sayısı, pazar payı dağılımları ve kripto para birimlerinin cirosu değerlendirilmiştir. Yapılan tüm bu değerlendirmeler sonucunda kripto paranın fiyatının, arz ve talep dinamikleri tarafından belirlendiği açıkça ifade edilmiştir. Aynı zamanda sistemin bir kaç istatistiki özelliklerinden hareketle, aktif kripto para birimleri sayısı da dahil olmak üzere, son bir kaç yıl boyunca kripto para biriminin istikrarlı olduğu ancak buna rağmen piyasa değerinin zaman içerisinde katlanarak arttığı sonucuna ulaşılmıştır.

Pichl ve Kaizoji (2017), Bitcoin'in kripto para birimi piyasalarının toplam kapitalizasyonunda en büyük paya sahip olduğunu ifade etmişlerdir. Bitcoin'in bu önemi itibariyle çalışma kapsamında Bitcoin fiyatlarının yanı sıra standart para birimlerinin de oynaklıkları ele alınmıştır. Aynı zamanda Bitcoin'in logaritmik getiri

dağılımı özellikleri ve arbitraj olanaklarından ekonometrik özelliklerine kadar çeşitli bakış açılarıyla inceleme yapmışlardır. Analizi gerçekleştirmek amacıyla 1 saniye, 1 dakika, 5 dakika, 1 saat ve son olarak 1 günlük örnekleme frekanslarını kullanmışlardır. Çalışmada işlem hacmi dağılımı için Kraken piyasasından alınan 17.05.2017 ile 12.08.2017 dönemleri arasındaki 88 günlük verileri inceleyerek Bitcoin Euro endeksini ifade eden BTCEUR üzerine inceleme yapmışlardır. Diğer yandan çalışmada Bitcoin piyasasında arbitraj fırsatlarını incelemek amacıyla 08.02.2013 ve 07.04.2017 tarihleri arasındaki 1 saatlik ölçekler doğrultusunda XBTEUR, XBTUSD, XBTCNY ve EURUSD ile son olarak USDCNY üzerinde inceleme yapılmıştır. Çalışma kapsamında yapılan tüm bu analizler sonucunda Bitcoin fiyatlarının diğer döviz kurlarından çok daha değişken olduğu sonucuna ulaşılmış ve gerçek işlem ücretleri durumunda arbitraj olanaklarının olabileceği gösterilmiştir.

Bouoiyour ve Selmi (2016), Bitcoin'in bugüne kadar bilinen en iyi dijital para birimi olarak kabul edilmesine karşın genel olarak bir varlık ve bağımsız bir elektronik para birimi olarak çok fazla değişkenlik gösterdiğine bu sebepten dolayı da fazlasıyla eleştiri aldığına dikkat çekilmiş ve çalışmalarını bu yönde şekillendirmişlerdir. Bouoiyour ve Selmi, çalışmalarında ilk dönem olarak 1 Aralık 2010 ve 31 Aralık 2014 dönemini, ikinci dönem olarak da 1 Ocak 2015 ve 20 Temmuz 2016 dönemini ele alarak Bitcoin fiyatlarını iki ana dönemde incelemişler ve farklı bilgi kriterleri ile seçilen optimal bir GARCH modeli kullanılmışlardır. Model çerçevesinde gerçekleştirilen analiz sonucunda özellikle ilk dönem içerisinde Bitcoin fiyatının ikinci döneme göre çok daha fazla değişkenlik gösterdiği anlaşılmıştır. Bu sonuçla birlikte ise düşük oynaklık oranına ulaşılmasına rağmen Bitcoin pazarının olgunlaşmadan uzak kaldığı yönünde yorumda bulunmuşlar ve bunuda Bitcoin sisteminin sahip olduğu risklere bağlamışlardır.

Fabian, Ermakova ve Sander (2016), Bitcoin'in merkezi olmayan ve dönüştürülebilir bir sanal para birimi olduğu ve düşük işlem maliyetleriyle işlem görürken bu işlemlerde aracı olarak faaliyet gösteren hiçbir finansal yapının olmadığı ifade edilmiştir. Yazarlar araştırmalarında Bitcoin ağı tarafından sağlanan anonimlik seviyesinin nasıl değerlendirildiğini, Bitcoin kullanıcılarının anonimliğin ne derece farkında olup endişelendiğini değerlendirmişlerdir. Çalışma kapsamında 125 aktif kullanıcı ile yapılan araştırmada 10 kişiden 7'sinin Bitcoin ağı ile orta veya yüksek

düzeyde anonimliği ilişkilendirdiğini ve bunların kaygılarını düşük ve orta olarak değerlendirdiğini ortaya koymuşlardır. Aynı zamanda katılımcıların %35'inin blockchain'i anonimleştirme riskinin farkında olmasına rağmen endişe duymadığını ancak %50'sinin ise endişe duyduğunu belirtmişlerdir. Katılımcıların yaklaşık üçte birinin özel anonimleştirme tekniklerinden habersiz olduğu da çalışmada dikkat çeken noktalar arasında gösterilmiştir. Araştırmaların sonucunda blokzincir teknolojisinin ve Bitcoin ağının anonimlik seviyesini artırmak için çaba sarf edilmesi gerektiği ve tam bir gizliliği garanti etmede zayıf yönlerinin olduğundan dolayı mevcut sistemi iyileştirme önlemlerinin alınması gerektiği yönünden tavsiyelerde bulunulmuştur.

Atik, Köse ve Yılmaz (2015), çalışmalarında Bitcoin'in diğer para birimleriyle olan ilişkilerini incelemeye çalışmışlar ve bunun için dünyada en yaygın olarak kullanılan para birimlerini veri olarak kullanmışlardır. Bu para birimlerini çapraz kur içerisinde önemli bir yere sahip olan EUR, GBP, JPY, CAD, AUD ve CHF olarak belirlemişler ve çalışmalarını bu doğrultuda şekillendirmişlerdir. Çalışmada, Bitcoin'in 2009 yılında ortaya çıkmasından dolayı Haziran 2009 ve Şubat 2015 dönemleri arasındaki Bitcoin'in dolar cinsinden günlük değerlerini incelemişlerdir. Ancak Bitcoin, 2013 yılında dalgalanmalar göstermeye başladığından dolayı 1 Nisan 2013 tarihinden sonraki verileri baz alarak analiz yapmışlardır. Yapılan analizle birlikte JPY, CAD ve AUD arasında pozitif yönlü güçlü bir ilişkinin olduğu; ancak EUR ve JPY arasında bu durumun tam tersi negatif yönlü güçlü bir ilişkini olduğu ortaya çıkarılmıştır. Aynı zamanda çalışmada yapılan Johansen eşbütünleşme testi sonucunda değişkenler arasında uzun dönemli bir ilişkinin olduğu sonucuna ulaşılmıştır.

Bartos (2015), kripto para birimini yenilikçi özelliklere sahip yeni ekonomik ve finansal araçlar şeklinde tanımlamıştır. Çalışmada yüzlerce farklı türde kripto para birimi olmakla birlikte en popülerlerinin Bitcoin, Litecoin, Dogecoin ve Ripple olduğu dile getirilip analiz kapsamında Bitcoin'e odaklanılmıştır. Kamuya açıklanmış bilgilerin hem Bitcoin fiyatı üzerindeki etkisi analiz edilmiş hem de Bitcoin fiyatının etkin pazar hipotezini yansıtma durumu tahmin edilmiştir. Bu doğrultuda Mart 2013'den Ağustos 2014'e kadarki günlük veriler ile hata düzeltme modeli metodolojisi kullanılmıştır. Analiz, Bitcoin gibi kripto para birimleri fiyatının, kamuya açıklanmış bilgilere tepki verdiğini ve etkin piyasaların hipotezini takip ettiğini doğrulamıştır. Diğer yandan analiz ile birlikte arz ve talep faktörlerinin

Bitcoin fiyatları üzerinde çok önemli bir etkisi olduğu anlaşılırken analiz; küresel ekonominin, finansal gelişmelerin ve yatırımcıların spekülasyonlarının Bitcoin fiyatını yükseltebileceği konusundaki önceki bulguları desteklememiştir.

Hayes (2015), kripto para ile üretim maliyet modellerine ilişkin ampirik bir analiz gerçekleştiren bu çalışmada Bitcoin'in popülaritesinin giderek artmasının Bitcoin'in değer oluşumunu etkileyen faktörlerin anlaşılmasını daha da önemli hale getirdiği söylenmiştir. Aynı zamanda Bitcoin'in fiyatlarındaki dalgalanmaların Dolar, Euro ve Çin Yuanı gibi ulusal para birimlerine göre son derece değişiklik gösterdiği de ifade edilmiştir. Değer oluşumlarının bu kadar etkili olmasına bağlı olarak çalışmada kripto para birimlerinin piyasada sergilemiş oldukları değer kaynakları tanımlanmaya çalışılmıştır. Bu doğrultuda bir regresyon modeli tahmin edilmiş ve kesitsel veri analizleriyle konu açıklanmaya çalışılmıştır. Bunun sonucunda kripto para birimlerinde nispi değer oluşumlarının nedenlerinin tanımlanmasında üretim marjının maliyetlerinin ana belirleyiciler olduğu sonucuna ulaşılmıştır.

Gandal ve Halaburda (2014), kripto para birimleri arasındaki döviz kurunda meydana gelen değişimleri incelemişlerdir. Bu doğrultuda bir yandan ağ etkilerinin farklı para birimleri ve bu paraların işlem gördüğü borsalar arasındaki rekabet gücünü analiz ederken diğer yandan arbitraj fırsatı bulunup bulunmadığını incelemişlerdir. Bunun sonucunda her iki ortamda da ağ etkilerinin önemli bir rol oynadığı anlaşılırken borsalar için herhangi bir arbitraj fırsatı bulunup bulunmadığına dair net bir bilgi elde edilememiştir. Çalışmada veriler Mayıs 2013-Eylül 2013 ve Ekim 2013-Şubat 2014 olmak üzere iki farklı döneme ayrılmıştır. İlk dönemde Bitcoin'in fiyatı daha istikrarlıyken ikinci dönemde çok daha fazla değişkenlik gösterdiği anlaşılmıştır. Aynı zamanda ilk dönem içinde Bitcoin'in popülaritesinin USD ve diğer kripto para birimleri karşısında arttığı tespit edilirken ikinci dönemde diğer kripto para birimlerinin fiyatının USD karşısında Bitcon'den daha fazla arttığı tespit edilmiştir. Diğer yandan ikinci dönemde, Bitcoin ve Litecoin arasında daha doğrudan bir rekabet olduğu gözlemlenmiştir. Dolayısıyla çalışmada hem korelasyon hem de Granger nedensellik testlerinden elde edilen sonuçlar doğrultusunda ikinci dönemde döviz kurları arasında daha fazla etkileşim olduğu anlaşılmıştır.

Gibbs ve Yordchim (2014), Litecoin'in elektronik ortamda oluşturulan ve tutulan, eşler arası bir kripto para birimi ve açık kaynaklı bir yazılım projesi olduğuna değinilmiştir. Gibbs ve Yordchim'e göre Litecoin'in Bitcoin'i iyileştirerek bir kaç

anahtar fark yaratmayı amaçlamıştır. Bu doğrultuda Litecoin'in daha hızlı işlem onayı sağlayıp her 2,5 dakikada bir blok işlemeyi hedefleyerek Bitcoin'in 1 saatte tamamladığı onaylama işlemini 20 dakikada tamamladığı ancak bunun blokzincir boyutunun ve artık blokların artmasına neden olup bir dezavantaj sergilediği belirtilmiştir. Diğer yandan Bitcoin ile aynı dönemde yapılan çifte harcama saldırısına karşın daha fazla direnç içermesinin Litecoin açısından büyük bir avantaj olduğuna dikkat çekilmiştir. Çalışmada analiz kapsamında Tayland içerisindeki Litecoin değerinin başarısını etkileyen faktörler analiz edilmeye çalışılmış ve bu doğrultuda 119 farklı kişiye anket uygulaması ve küçük grup tartışmalarıyla röportaj yapılmıştır. Analizleri sonucunda Bitcoin'in daha yüksek bir algılama değerine sahip olduğu, Litecoin'in gelişiminde işbirliğinin teşvik edilmesi ve halkın Litecoin konusunda bilgi seviyesinin artırılması gerektiği anlaşılmıştır.

Vejačka (2014), Bitcoin'in sıradan kullanıcılar ve Bitcoin madencileri olmak üzere iki farklı kullanıcısının olduğu ifade edilmiştir. Bu noktada normal Bitcoin kullanıcıları, elektronik bankacılık uygulamalarına benzer dijital yazılım yöntemi olan cüzdanları kullanan ve bu şekilde ödeme işlemlerini gerçekleştiren kullanıcılar olarak tanımlanmıştır. Normal Bitcoin kullanıcıları tarafından kullanılan bu cüzdanlardaki dosyaların ise, özel anahtar sahibi ile sınırlı olmasına bağlı olarak, kaybolma ya da silinme gibi durumlarda sonsuza kadar yok olacağına dikkat çekilmiştir. Diğer yandan bir diğer Bitcoin kullanıcı türü olan madencilerin ise hesaplama güçlerini Bitcoin ağına dayandırarak yapay matematiksel problemleri çözen, bekleme işlemelerini blokzincire dahil ederek onaylama işlemlerinde kullanan ve blok yaratan kullanıcılar olduğu ifade edilmiştir. Bu aşamada ise Bitcoin'in SHA2-256 algoritmasını Litecoin'in Scrypt algoritmasını kullanıp işlem onayını hızlandırdığına dikkat çekilmiştir. Çalışmada uygulama kapsamında ise Bitcoin'in ve Litecoin'in volatilitesi incelenmiş ve ana borsa endeksleri, emtialar ve Euro para çifti ile karşılaştırılmıştır. Bu kapsamda kripto para birimlerinin temel endekslerden ve yatırım araçlarından çok daha yüksek seviyelerde volatiliteye sahip olduğu doğrulanmıştır.

3. 2. KRİPTO PARA VE DÖVİZ KURU İLİŞKİSİNE EKONOMETRİK BİR YAKLAŞIM

Çalışmanın bu başlığı altında kripto para Bitcoin ile döviz kuru arasında ilişki analiz edilmiştir. Bu bağlamda analize yönelik teorik altyapısına değinilip analiz sonuçları verilmiştir.

3. 2. 1. Analizde Kullanılan Ekonometrik Yönteme İlişki Teorik Altyapı

Bu kısımda, yapılan analizin ve elde edilen sonuçların net bir şekilde anlaşılabilmesi amacıyla, uygulanan ekonometrik analiz yöntemleri teorik olarak ayrıntılı bir şekilde açıklanmıştır.

3. 2. 1. 1. Birim Kök Testi

Birim kök kavramı açıklanmadan önce durağanlık kavramının ne olduğunun bilinmesi gerekmektedir. Durağanlık kavramı sabit ortalama, sabit varyans ve seriye ait iki değer arasındaki farkın zaman farkına bağlı olarak değil yalnızca iki zaman değeri arasındaki farka bağlı olması şeklinde tanımlanmaktadır. Literatürde zamandan etkilenmeyen, ortalaması, varyansı ve kovaryansı sabit olan seriler zayıf durağan (weakly stationary) olarak adlandırılmaktadır. Güçlü durağanlıkta (strongly stationary) ise sonlu ortalamalı ve varyansa gerek olmamaktadır. Bu iki durağanlık kavramı karşılaştırıldığı zaman zayıf durağanlığın daha kısıtlı şartlar taşıdığı görülmektedir. Bu noktada herhangi bir Y_t serisinin durağan olma şartları ise aşağıdaki denklemde özetlenmiştir. Denklem, bütün t değerleri için k gecikme mesafesini göstermektedir (Uzgören ve Uzgören, 2005: 3).

Sabit Aritmetik Ortalama $: E(Y_t) = \mu$ (6)

Sabit Varyans $: Var\,(Y_t) = E\,(Y_t - \mu)^2 = \sigma^2$ (7)

Gecikme Mesafesine Bağlı Kovaryans $: Y_k = E[(Y_t - \mu)(Y_{t-k} - \mu)]$ (8)

Zaman serisinin durağanlığının test edilmesinde korelogram testinden ve birim kök (unit root) testinde yararlanılmaktadır. Analizlerde en sık kullanılan teknik birim kök testi olmakla birlikte bu noktada iki farklı değişkenle ilgili zaman serilerinin regrese edildiği durumda aralarındaki ilişkinin sahte ya da gerçek olup olmadığına dikkat edilmesi gerekmektedir. Çünkü durağan olmayan zaman serileriyle yapılan çalışmalarda sahte regresyon ortaya çıkabilmektedir. Sahte regresyon durumunda yüksek R^2 ve anlamlı T istatistik değerleri söz konusu olsa bile parametre tahminleri ekonomik olarak anlamsız olmaktadır. Dolayısıyla eğer durağan olmayan zaman serilerinin kullanılmasıyla analiz gerçekleştirilirse tahmin edilen modelde yer alan tüm değişkenler arasındaki ilişki gerçekten bağımsız ve hatalı olabilmektedir. Bundan dolayı çalışmalarda zaman serisi analizi gerçekleştirileceği zaman sahte regresyondan kaçınabilmek için kullanılan zaman serilerinin durağanlığının test edilmesi ve kaçıncı seviyede durağan olduğunun belirlenmesi gerekmektedir (Ayvaz Güven ve Ayvaz, 2016: 247).

Bu noktada birim kökün varlığı test edilirken dikkat edilmesi gereken bazı önemli noktalar bulunmaktadır (Uçan, 2019: 182). Bunlar:

- Veri türetme işleminin stokastik ya da deterministik bir zaman trendi içerme olasılığı dikkate alınmalıdır.
- Veri türetme işlemi basit bir otoregresif (AR (1)) süreçten daha karmaşık olarak hareketli ortalama (MA) terimleri içerebilmektedir.
- Sonlu örneklemlerde uygulanan teste bağlı olarak durağan bir seri eğer birim kök içermeye yakın ise, seri durağan iken, uygulanan test durağan olmadığı yönündeki sıfır hipotezi kabul edilebilmektedir.
- Serideki tespit edilemeyen yapısal kırılmalar durağanlığın belirlenmesinde hatalı sonuçlar çıkarabilmektedir.

Birim kök testi için kullanılan otoregresif model ise aşağıda gösterilmiştir (Ümit, 2007:160):

$$Y_t = PY_{t-1} + u_t \qquad (9)$$

Denklemde (u_t) beyaz gürültü (white-noise) olarak bilinmekle birlikte stokastik bir hata terimini yani ortalaması sıfır, varyansı (σ^2) değişmeyen ve ardışık bağımlı olmayan olasılıklı hata terimini; (Y_t) Y'nin t zamanında aldığı değeri ve (Y_{t-1}) Y'nin t zamanından bir önceki dönemde aldığı değeri ifade etmektedir. Bu model birinci dereceden otoregresif AR(1) modelidir. Eğer bu tahmin edilen regresyonda (Y_{t-1})'in katsayısı olan (*P*) bire eşit (*P*=1) ise analizde birim kök sorunu ortaya çıkmaktadır. Bu durum zaman serisi analizlerinde rassal yürüyüş (random walk) olarak ifade edilmekte ve serinin durağan olmadığı anlamına gelmektedir. Bununla birlikte ise model aşağıdaki şekli almaktadır:

$$Y_t = Y_{t-1} + u_t \qquad (10)$$

Bu durum bir önceki dönemde iktisadi değişkenin değerinin ve o dönem içerisinde maruz kaldığı şokun olduğu gibi sistemde kaldığını ifade etmektedir. Bu durumun bütün bir dönem için geçerli olduğu düşünülünce, durumlar bütün bir dönem için geçerli olmakta ve daha önceki dönemlerde de ortaya çıkan şokların da değişkenin bu dönemdeki değerine etkisinin sürdüğü ve buna bağlı olarak geçmişteki tüm şokların toplamın oluştuğu anlamına gelmektedir. Bu şokların kalıcı olması ise serinin durağan olmaması ve zaman içerisinde gösterdiği trendin stokastik olmasını ifade etmektedir. Burada *P* katsayısı birden küçük çıkarsa, geçmiş dönemlerde ortaya çıkan şoklar belirli bir süreliğine etkisini sürdürmüş olsalar da, bu etki zaman içerisinde giderek azalacağı ve kısa bir dönem sonra tamamen ortadan kalkacağı anlamına gelmektedir (Tarı, 2015: 388).

Yukarıda verilen 9 nolu otoregresif denklemin sağ ve sol olmak üzere her iki tarafından Y_{t-1} çıkarılırsa,

$$Y_t - Y_{t-1} = PY_t - Y_{t-1} + u_t \text{ veya } \Delta Y_t = (P-1)\,Y_{t-1} + u_t \qquad (11)$$

İlişkisi elde edilmektedir. Burada $\Delta Y_t = Y_t - Y_{t-1}$ birinci farktır. Denklemde (*P*-1) eğer δ olarak ifade edilirse ilişki,

$$\Delta Y_t = \delta Y_{t-1} + u_t \quad (12)$$

olarak sembolize edilmektedir. (P = 1) olduğunda (δ = 0) olacaktır. (δ = 0) olduğunda ise,

$$\Delta Y_t = Y_t - Y_{t-1} = u_t \quad (13)$$

olacaktır. Dolayısıyla (Y_t) birinci fark durağan olacaktır (Yeşilyurt, 2019: 97). Bir zaman serisinin durağan olduğu seviyenin test edilmesinde kullanılan hipotezler ise aşağıdaki gibidir:

$$H_0 : \delta = 0 \text{ ve } P = 1$$
$$H_1 : \delta \neq 0 \quad (14)$$

H_0 hiptezi (Y_t) zaman serisinin durağan olmadığını dolayısıyla normal dağılmadığını ve otokorelasyona sahip yani birim kök içerdiğini ifade etmektedir. H_1 hipotezi ise (Y_t) zaman serisinin durağan olup normal dağıldığı ve otokorelasyona sahip olmayıp birim kök içermediği anlamına gelmektedir (Bağdiken ve Beşer, 2009: 6).

Orijinal bir seri farklı seviyelerde durağan olabilmektedir. Zaman serisi I(0) ise bu serinin seviyede durağan olduğu anlamına gelmektedir. Ancak eğer seri birinci farkında durağan ise bu orijinal seriye birinci dereceden entegre olmuş denilmektedir. Bu sembolik olarak I(1) biçiminde ifade edilmektedir. Eğer seri iki defa fark alındıktan sonra durağan olduğu tespit edilirse bu serinin ikinci seviyede durağan yani I(2) olduğu anlamına gelmektedir. Aynı şekilde d defa fark alınarak durağan olduğu tespit edilen bir seri d'inci dereceden entegre edilmiş sayılmakta ve I(d) olarak yazılmaktadır. Bu durumlarda, durağan olmayan bir seri, farkları alınarak durağan hale getirilebilmektedir. Yani bir serinin durağan olmadığı durumlarda birinci dereceden veya daha yüksek dereceden farkları alınarak entegre bir zaman serisi haline getirilebilmektedir. Gerçekleştirilen bu işlem, serinin içerdiği kalıcı şokun

etkisinin ortadan kaldırılmasını ve durağan yani belli bir değere yaklaşan geçici şokların kalmasını dolayısıyla serinin durağan hale gelmesini sağlamaktadır. Ancak serinin I(0) olduğu durumda yani orijinal serinin zaten durağan bir yapıda fark almaya gerek yoktur (Tarı, 2015: 388-389).

Bu noktada bir serinin durağan olup olmadığının birim kök testiyle araştırılmasında kullanılan yöntemlerin açıklanması gerekmektedir. ($H_0 : \delta = 0$) olması serinin durağan olmadığı anlamına gelmektedir. (P=1) sıfır hipotezi doğrultusunda geleneksel yolla hesaplanan t istatistiği hesaplanmamaktadır. Çünkü H_0 hipotezinde t istatistiğinin tutarlı olması için serilerin durağan olması gerekmektedir. Yani bunun en önemli nedeni t testinin sıfır etrafında dağılmıyor olmasıdır. Bundan dolayı t istatistiği yerine τ (tau) istatistiği kullanılmaktadır. Bu istatistik literatürde Dickey Fuller (DF) sınaması olarak bilinmektedir. Diğer yandan bu istatistiğin kritik eşik değerini gösteren tablo Dickey-Fuller tarafından Monte Carlo benzetimleriyle çizelgeleştirilmiştir. Ancak zamanla bu çizelgelerin yeterli olmadığı anlaşılarak Mac Kinnon tarafından genişletilmiştir. Dolayısıyla hesaplanan DF test istatistiğinin mutlak değeri ($|\tau|$) DF'nin veya Mac Kinnon DF'nin mutlak eşik değerinden küçük ise ($H_0 : \delta = 0$ ve $P = 1$) hipotezi kabul edilmekte ve incelenen serinin durağan olmadığı yani birim kök içerdiği sonucuna ulaşılmaktadır. Eğer hesaplanan τ istatistiği DF'nin ya da Mac Kinnon DF'nin mutlak değer eşiğinden küçükse ($H_0 : \delta = 0$ ve $P = 1$) hipotezi reddedilirken alternatif hipotez olan ($H_1 : \delta \neq 0$) hipotezi kabul edilmektedir. Bu durum incelenen serinin durağan olduğu ve birim kök içermediği anlamına gelmektedir (Ümit, 2007: 161).

Teori ve uygulama yönünden farklı nedenlerle, Dickey-Fuller testi şu regresyonlara uygulanmaktadır:

Sabitsiz ve trendsiz regresyon $: \Delta Y_t = \delta Y_{t-1} + u_t$ (15)

Sabitli ve trendsiz regresyon $: \Delta Y_t = \beta_0 + \delta Y_{t-1} + u_t$ (16)

Sabitli ve trendli regresyon $: \Delta Y_t = \beta_0 + \beta_1 t + \delta Y_{t-1} + u_t$ (17)

bulunarak, bunlarla birlikte (tau) veya DF istatistikleri MacKinnon kritik değerleri elde edilmektedir. Eğer (u_t) hata terimi otokorelasyonlu ise (17) nolu denklem,

$$\Delta Y_t = \beta_0 + \beta_1 t + \delta Y_{t-1} \alpha_i \sum_{i=1}^{m} \Delta Y_{t-i} + u_t \quad (18)$$

biçiminde düzenlenmektedir. Burada gecikmeli fark terimleri kullanılmaktadır. Bu gecikmeli fark terimlerinin sayısı ise çoğunlukla ampirik olarak belirlenmektedir. Buradaki ana fikir (18) numaralı denklemdeki hata teriminin otokorelasyonsuz olmasını sağlayacak kadar terimi modele katmaktır. Burada H_0 hipotezi ($P = 1$) veya ($\delta = 0$) olup Y'de birim kök olduğunu yani durağan olmadığını ifade etmektedir. Yukarıdaki bahsedilen DF sınamasında ele alınan bütün regresyonlar birinci dereceden otoregresif süreçleri AR (1) ifade etmektedir. Ancak (18) numaralı denklemdeki gibi modellere eğer DF testi uygulanırsa buna Genişletilmiş Dickey-Fuller (Augmented Dickey Duller) testi denilmektedir. Bu kısaca ADF testi olarak da bilinmektedir. Her iki test istatistiğinin kritik değerleri ise aynıdır (Yeşilyurt, 2019: 98-99).

AR (1) sürecinde olduğu gibi, AR (d) sürecini ifade eden regresyon modeli sabit terim ve lineer zaman trendi eklenerek genişletilmiş hali ve dolayısıyla ADF testi için üç ayrı regresyon denklemi aşağıda gösterilmiştir:

$$\Delta Y_t = \delta Y_{t-1} + \alpha_i \sum_{i=2}^{m} \Delta Y_{t-i+1} + u_t \quad (19)$$

$$\Delta Y_t = \beta_0 + \delta Y_{t-1} + \alpha_i \sum_{i=2}^{m} \Delta Y_{t-i+1} + u_t \quad (20)$$

$$\Delta Y_t = \beta_0 + \beta_1 t + \delta Y_{t-1} + \alpha_i \sum_{i=2}^{m} \Delta Y_{t-i+1} + u_t \quad (21)$$

Hesaplanan test istatistikleri; ilk modelde (19) sabitsiz ve trendsizdir. İkinci modelde (20) modele sadece sabit eklenmekte ve model sabitli ve trendsiz olmaktadır. üçüncü modelde (21) ise modele hem sabit hem de trend eklenerek model sabitli ve trendli olmaktadır. ADF testi bağımlı değişkenin gecikmeli değerlerini kullanarak otokorelasyonu ortadan kaldırmayı hedeflediğinden dolayı gecikme uzunluğunun belirlenmesi en önemli unsurlardan biridir. Çünkü gecikme uzunluğunun çok az sayıda olması doğru hipotezin reddedilmesine neden olurken çok fazla sayıda olması da testin gücünü azaltmaktadır.(Yıldırım, 2010: 24).

Genellikle uygun gecikme uzunluğunun belirlenmesinde Akaike bilgi kriteri (AIC) ve Schwartz bilgi kriteri (SC) olmak üzere iki temel kriter kullanılmaktadır. Bunlar aşağıda gösterilmiştir (Gökçe, 2015: 38):

$$\text{AIC (m)} = \ln \left| \sum e\ (m) \right| + \frac{2}{T} = \ln \left| \sum e\ (m) \right| + \frac{2mK^2}{T} \quad (22)$$

AIC minimum ortalama hata kareyi kullanmaktadır. Uygun gecikme sayısı AIC değerinin minumum olmasını sağlayan p değeridir.

$$\text{SC (m)} = \ln \left| \sum e\ (m) \right| + \frac{lnT}{T} \text{mK}^2 \quad (23)$$

SC değerinin minumum yapan p değeri uygun gecikme sayısı olarak belirlemektedir.

DF testlerinin dağılım teorisi hataların istatistiksel olarak bağımsız ve sabit varyansa sahip olduklarını varsaymaktadır. Dolayıısyla DF testleri kullanıldığında hataların korelasyonsuz ve sabit varyansa sahip olduğundan emin olunması gerekmektedir. Ampirik ekonometrik çalışmaların büyük bir çoğunluğunda

bağımsızlık ve sabit varyans varsayımları hatalarla ilgili güçlü varsayımlar olarak nitelenmektedir. Ancak rassal yürüyüş süreci olarak nitelendirilen zaman serilerinde bu varsayımların yanlış olduğuna inanılması için iktisadi teoride fazlasıyla iyi nedenler bulunmaktadır. Philips ve Perron ise bu varsayımlara karşın alternatif bir birim kök testi ortaya çıkarmışlardır. Philips ve Perron'un geliştirdikleri bu testle fazlasıyla genel, zayıf bağımlı ve benzer dağılmayan kalıntılara izin veren birleşik t istatistik regresyonu ve EKK tahmin edicileri için asimptotik bir teori sağlamışlardır. Philips-Perron (PP) testi bu bağlamda ADF testinin bir dönüşümü olup, parametrik olmayan yöntem kullanarak, bu dönüşüm sorunlu parametrenin bağımlılığını asimptotik olarak ortadan kaldırmaktadır (İğde, 2010: 19). PP testi DF testindeki regresyon denklemini aynen kullanmakla birlikte denklemdeki bir önceki resime ait parametrenin (δ) tau (τ) istatistiğinde parametrik olmayan düzeltme yaparak, otokorelasyon sorununu çözmektedir. Testlerin eşik değerleri ise birbirleriyle aynı kalmaktadır (Çelik ve Taş, 2007: 16).

Hata teriminin zayıf derecede bağımlı olmasına ve heterojen olmasına dayan PP testinin regresyonları aşağıda gösterilmiştir (Akıl, 2019: 29):

$$Y_t = \mu + \alpha Y_{t-1} + \varepsilon_t \tag{24}$$

$$Y_t = \mu + \alpha Y_{t-1} + \beta\left(t - \frac{T}{2}\right) + \varepsilon_t \tag{25}$$

Denklemde (T) gözlem sayısı, (α) ve (β) katsayılar, (ε_t) ise beklenen değeri sıfıra eşit hata terimlerinin dağılımını sembolize etmektedir. Burada hata terimleri arasında içsel bağlantının olmadığı ya da homojenlik varsayımı gerekli değildir.

PP testi için hipotezler ise aşağıda verilmiştir:

$$H_0 : P = 0$$
$$H_1 : P < 0 \tag{26}$$

H_0 hipotezi seri durağan değildir ve seride birim kök vardır varsayımına dayanmaktadır. H_1 ise seri durağan ve birim kök yoktur varsayımına dayanmaktadır. PP birim kök testi istatistiklerinde, ADF test istatistiği için kullanılan kritik tablo değerleri karşılaştırılarak hipotez kabul ya da reddedilmektedir. Elde edilen sonuçlar doğrultusunda da serinin durağan olup olmadığına karar verilmektedir. Burada özellikle trend içeren serilerde, MA süreçlerinin artması durumunda PP testi, DF testiyle kıyaslandığında, daha güçlüdür. MA süreçlerinin negatif olması durumunda ise ADF testleri, PP testlerine göre daha güçlüdür. Burada MA süreçlerinin negatif ya da azalan olması hata terimlerinin beklenen ortalamasının sıfıra yaklaşması demektir. PP testi, veri yaratma sürecinin MA pozitif özelliğini göstermesi durumunda güçlüdür.

3. 2. 1. 2. Eşbütünleşme Analizi: ARDL Sınır Testi Yaklaşımı

Eşbütünleşme durağan olmayan iki zaman serisi arasındaki korelasyonu incelemek amacıyla kullanılmaktadır. Eğer birden fazla zaman serisi kendileri durağan olmadıkları halde, doğrusal kombinasyonları durağan ise bu serilerin eşbütünleşik oldukları anlamına gelmektedir. İktisadi anlamda ise bu seriler arasında uzun dönem durağan olmayan zaman serileri üzerine analiz yapmışlardır. Ancak bu durumda sahte regrasyon sorunuyla karşı karşıya kalınmış ve bu durumu Clive Granger ile Robert Engle (1987) tarafından ispatlanmıştır. Burada sahte regresyon ise durağan olmayan zaman serilerinin içerdiği stokastik eğilim etkisinden kaynaklanmaktadır. Stokastik eğilim etkisi önemsenmeden yapılan regresyonlarda iki seri arasında olmayan ilişkiler varmış gibi görünürken bu ilişki rastlantısal olarak gelişen bir eğilime dayanmaktadır. Bu bilgiler beraberinde mevcut niceliksel çalışmaların tekrar gözden geçirilmesini getirmiştir (Uçan, 2019: 187).

Bu bağlamda eşbütünleşme kavramı basit bir model üzerinde aşağıdaki gibi açıklanabilmektedir:

$$Y_t = \alpha + \beta X_t + u_t \qquad (27)$$

(27) nolu denklemde (Y_t) ve (X_t) serileri durağan değilse ortaya sahte regresyon durumu çıkmaktadır. Buna bağlı olarak da T ve F istatistik sonuçları doğru bir sonuç ortaya çıkaramamaktadır. Literatürde eşbütünleşme analizinde ise en çok başvurulan yöntem Engle-Granger ve Johansen-Juselius testleri olduğu görülmektedir. Ancak bu eşbütünleşme testlerinde tüm serilerin aynı seviyede durağan olması gerekmektedir. Bu durumda analizin gerçekleştirilmesinde bir tür dezavantaja neden olabilmektedir (Ballı, 2019: 74).

Eşbütünleşmeye ARDL analizi yaklaşımının en önemli avantajlarından biri bu noktada kendini göstermektedir. Çünkü ARDL analizi değişkenlerin hepsinin seviyede I(0) veya birinci farkında I(1) durağan olduğu durumun yanı sıra bazı değişkenlerin I(0) bazı değişkenlerinde I(1) olduğu durumlardan bağımsız olarak analiz yapılmasına olanak sağlamaktadır. Bir diğer ifadeyle ARDL analizi değişkenlerin farklı seviyelerde durağan olduğu durumda, seriler arasında uzun dönemde eşbütünleşme ilişkisi olup olmadığının sınanmasında da kullanılabilmektedir. Ayrıca, tüm değişkenlerin içsel kabul edilmesi, küçük örneklem durumlarında yani gözlem sayısının sınırlı olduğu durumlarda sapmasız ve tutarlı sonuçlar elde edilmesine imkân sağlamaktadır. Araştırmaya konu olan değişkenler arasında hem kısa hem de uzun dönemli ilişkilerin eşanlı olarak test edilmesine olanak sağlaması da, diğer analiz yöntemleriyle kıyaslandığında, ARDL analizine avantaj kazandıran özellikler arasında bulunmakta ve daha güvenilir sonuçlar ortaya çıkarmaktadır (Özaydın, 2018: 145).

ARDL analizi kapsamında uzun dönemli ilişkinin varlığını test etmek için kullanılan test ise sınır testidir. ARDL sınır testi temelde üç aşamadan oluşmaktadır. İlk olarak analize dâhil edilen değişkenler arasında uzun dönemli ilişki olup olmadığı test edilmektedir. Eğer eşbütünleşme ilişkisi tespit edilirse sırasıyla uzun ve kısa dönem elastikiyetleri elde edilmektedir. Ancak ARDL analizinin yapılması için öncelikli olarak uygun gecikme uzunluğunun tespit edilmesi gerekmektedir. Daha sonra eşbütünleşme ilişkisinin test edilmesi için (H_0: $Q_1 = Q_2 = 0$) temel hipotezi F testi kullanılarak sınanmaktadır. Ancak bu temel hipotezi sınamak için kullanılan standart F testi, bazı durumlar için standart olmayan bir dağılıma sahiptirler. Bu durumlar literatürde; ARDL modelinde bulunan değişkenlerin I(0) veya I(1) olup olmaması, değişken sayısı, ARDL modelinin sabit veya trendli olup olmaması olarak ifade edilmektedir Bundan dolayı test istatistiği ile karşılaştırılması gereken kritik

değerler Peseran vd. (2001) tarafından tablolaştırılmıştır (Pamuk ve Bektaş, 2014: 82).

ARDL sınır testine ait hipotezler (28) nolu denklemde gösterilmiştir:

$$H_0 = \delta_1 = \delta_2 = \delta_3 = 0$$

$$H_1 : \delta_1, \delta_2, \delta_3 \neq 0 \qquad (28)$$

H_0 hipotezi değişkenler arasında uzun dönemli ilişki olmadığı varsayımına dayanırken alternatifi uzun dönemli ilişkinin varlığı yönündeki varsayımı kabul etmektedir. Burada değişkenler I(0) ve I(1) olma durumlarına göre alt ve üst sınırlar doğrultusunda kritik değerler belirlenmiştir. Eğer hesaplanan F istatistik değeri kritik değerin üst sınırından büyük ise değişkenler arasında uzun dönemli ilişki olmadığına yönelik hipotez reddedilmektedir. Ancak F istatistik değeri alt sınır değerinden küçük ise temel hipotez kabul edilmekte ve değişkenler arasında uzun dönemli ilişki olmadığı sonucuna ulaşılmaktadır. F istatistik değeri alt ve üst sınır aralığında ise bu durumda da herhangi bir karar alınamamaktadır (Çetin ve Şeker, 2014: 221).

3. 2. 1. 3. Vektör Otoregresyon (VAR) Modeli

İktisadi ilişkilerin karmaşık oluşu olayların çoğunun tek denklemli modeller yerine eşanlı denklemler aracılığıyla incelenmesine neden olmuştur. Ekonomik hayatta, makroekonomik değişkenlerin karşılıklı olarak birbirleriyle etkileşim halinde oldukları görülmektedir. Bundan dolayı verileri salt içsel ya da dışsal değişken olarak ayırmak zorlaşmaktadır. Bu noktada Sims'in 1980 yılında yazmış olduğu makale ile VAR analizi ileri sürülerek eşanlı denklem sistemlerinde içsel-dışsal değişken ayrımı gibi güçlüklere çözüm geliştirilmiştir. Ayrıca eşanlı denklem sistemlerinde, belirlenme problemini belirleme modelini aşabilmek için bazen yapısal model üzerine bazı kısıtlamalar yapılması zorunlu olmaktadır. Bu kısıtlamalar araştırma için bazı güçlükler ortaya çıkarmaktadır. VAR modeli bu noktada yapısal model üzerinde herhangi bir kısıtlama olmaksızın dinamik ilişkileri ortaya koyabilmektedir. Ayrıca VAR analizi bağımlı değişkenlerin gecikmeli değerlerinin yer alması, geleceğe dönük güçlü tahminlerin yapılmasına olanak sağlamaktadır (Tarı ve Bozkurt, 2006: 4-5).

Y ve X gibi iki değişken için basit bir VAR modeli:

$$Y_t = \alpha_{10} + \sum_{i=1}^{P} \alpha_{11i} Y_{t-i} + \sum_{i=1}^{P} \alpha_{12i} X_{t-i} + u_{1t} \quad (29)$$

$$X_t = \alpha_{20} + \sum_{i=1}^{P} \alpha_{21i} Y_{t-i} + \sum_{i=1}^{P} \alpha_{22i} X_{t-i} + u_{2t} \quad (30)$$

Burada, (α_{10}) sabit terim, α_{ijk} 'nci denklemdeki j'nci değişkenin k gecikmesine ait parametre, u_{it} hata terimi ve p gecikme sayısıdır. Denklemlerin sağ taraflarındaki değişkenler aynıdır. Bu vektör terimi iki veya ikiden daha fazla olan değişkenden oluşan vektörün ele alınmasında, otoregresyon teriminde bağımlı değişkenin gecikmeli değerinin denklemin sağında yer almasından gelmektedir. Sabit terim, modele değişkenlerin sıfırdan farklı olması durumunda dâhil edilmektedir (Tarı, 2015: 452).

VAR modeli matris gösterimi kullanarak ifade edilerek standart VAR denklemi haline getirilebilmektedir (Uçar, 2014: 36-37):

$$y_t + b_{12} z_t = b_{10} + Y_{11} y_{t-1} + Y_{12} z_{t-1} + \varepsilon_{yt} \quad (31)$$

$$b_{21} y_t + z_t = b_{20} + Y_{21} y_{t-1} + Y_{22} z_{t-1} + \varepsilon_{zt} \quad (32)$$

eşitlik matris formunda ifade edilirse,

$$\begin{bmatrix} 1 & b_{12} \\ b_{21} & 1 \end{bmatrix} \begin{bmatrix} y_t \\ z_t \end{bmatrix} = \begin{bmatrix} b_{10} \\ b_{20} \end{bmatrix} + \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix} \begin{bmatrix} y_{t-1} \\ z_{t-1} \end{bmatrix} + \begin{bmatrix} \varepsilon_{Yt} \\ \varepsilon_{zt} \end{bmatrix} \quad (33)$$

veya,

$$\beta x_t = \Gamma_0 + \Gamma_1 x_{t-1} + \varepsilon_t \quad (34)$$

elde edilir. Bu eşitlikte,

$$\beta = \begin{bmatrix} 1 & b_{12} \\ b_{21} & 1 \end{bmatrix}, x_t = \begin{bmatrix} y_t \\ z_t \end{bmatrix}, \Gamma_0 = \begin{bmatrix} b_{10} \\ b_{20} \end{bmatrix}, \Gamma_1 = \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix}, \varepsilon_t = \begin{bmatrix} \varepsilon_{Yt} \\ \varepsilon_{zt} \end{bmatrix} \quad (35)$$

değerleri ile ifade edilmektedir. VAR modeli β^{-1} ile standart formda yazıldığında ise aşağıdaki eşitlik elde edilmektedir:

$$x_t = A_0 + A_1 x_{t-1} + e_t \quad (36)$$

eşitliğinde yer alan değişkenler ($A_0 = \beta^{-1}\Gamma_0$,), ($A_1 = \beta^{-1}\Gamma_1$) ve ($E_t = \beta^{-1}\varepsilon_t$,) olmak üzere ($e_{1t}$)ve (e_{2t})şoklarının varyans-kovaryans matrisi aşağıdaki gibidir:

$$\sum = \begin{bmatrix} var(e_{1t}) & cov\,(e_{1t}, e_{2t}) \\ cov\,(e_{1t}, e_{2t}) & var(e_{2t}) \end{bmatrix} \quad (37)$$

$\sum$'nin tüm elemanları zamandan bağımsız olduğundan dolayı, $\sum$ aşağıdaki şekilde olacaktır:

$$\sum = \begin{bmatrix} \sigma_1^2 & \sigma_{12} \\ \sigma_{21} & \sigma_1^2 \end{bmatrix} \quad (38)$$

Buradan Var(e_{it})= σ_1^2 ve σ_{12}= σ_{21}= $cov\,(e_{1t}, e_{2t})$ eşitlikleri sağlanmaktadır. VAR modelinin geri dönüşümlü bir yapı içinde tahmin edilmesi modelin indirgenmiş biçim parametreleri ile tahmin edilmektedir.

Bu modellere ek olarak son zamanlarda ise özellikle parasal aktarım mekanizmasıyla ilgili konularda VAR modellinin yerine yapısal VAR (SVAR) modelleri kullanılmaktadır. SVAR modellerinin ortaya çıkmasında temelde mevcut VAR modelinin yapısal değişkenlerinin etkisini istenildiği gibi yansıtamamış olması etkili olmuştur (Adıgüzel, 2012: 104).

SVAR analizi iktisat teorisini kullanarak değişkenler arasındaki eşanlı ilişkileri ortaya koymaya çalışmaktadır. Bu doğrultuda (Uçar, 2014: 38),

$$y_t = b_{10} - b_{12}z_t + Y_{11}y_{t-1} + Y_{12}z_{t-1} + \varepsilon_{yt} \quad (39)$$

$$z_t = b_{20} - b_{21}y_t + Y_{21}y_{t-1} + Y_{22}z_{t-1} + \varepsilon_{zt} \quad (40)$$

eşitliği VAR modelinin yapısal biçimde gösterilişidir. Sistemi indirgenmiş forma dönüştürebilmek için,

$$y_t + b_{12}z_t = b_{10} + Y_{11}y_{t-1} + Y_{12}z_{t-1} + \varepsilon_{yt} \quad (41)$$

$$b_{21}y_t = b_{20} + Y_{21}y_{t-1} + Y_{22}z_{t-1} + \varepsilon_{zt} \quad (42)$$

eşitlikleri elde edilmiştir. Bu model indirgenmiş bir şekilde katsayıları ile ifade edildiğinde,

$$y_t = a_{10} + a_{11}y_{t-1} + + a_{12}z_{t-1} + e_{1t} \quad (43)$$

$$z_t = a_{20} + a_{21}y_{t-1} + + a_{22}z_{t-1} + e_{2t} \quad (44)$$

eşitlikleri elde edilmektedir. Bu eşitliklerden elde edilecek (e_{1t}) ve (e_{2t}) bağımlı değişkenlerin bir dönem sonrasına ilişkin hata tahminleridir.

VAR modelinde parametrelerin doğrudan yorumlanması çok anlamlı olmamaktadır. Bu nedenlerle analizin gerçekleştirilmesinde farklı testlerdende yararlanılmaktadır. Bu testler etki-tepki (impulse-response) analiz ve varyans ayrıştırması (variance decomposition) analizlerinden oluşmaktadır. Bu testler aracılığıyla net bir yorumlamaya ulaşılabilmektedir (Tarı, 2015:453).

Etki-tepki analizi, rassal hata terimlerinde birindeki standart sapmalık bir şokun, içsel değişkenlerin değerlerine olan etkisini yansıtmaktadır. Bu yansıtma şimdi ve geleceğe yönelik olmaktadır. VAR analizinde, değişkenler arasındaki dinamik etkileşimin ve simetrik ilişkilerin tespit edilmesinde etki-tepki fonksiyonu önemli bir yer tutmaktadır. Ayrıca makroekonomik büyüklüğün üzerinde en çok etkisi olan değişkenin politika aracı olarak kullanılabilme durumunun belirlenmesinde de etki-tepki analizi kullanılabilmektedir. Kısacası etki-tepki anakizi bir değişkende meydan gelen ya da gelebilecek bir değişimin diğer değişkenlerde nasıl bir etki meydana getireceğini göstermektedir. Bu analiz aynı zamanda değişkenin kendinde gelecek bir değişimin yine kendisi üzerinde ne gibi bir etkiye yol açacağını göstermesi açısından da önem taşımaktadır. (Sarı, 2008: 4).

Varyans ayrıştırması ise bağımlı değişkenlerin, diğer değişkenlere yönelik şoklara karşılık, kendi şokları nedeniyle meydana gelen hareketlerinin oranını ortaya koymaktadır. Yani varyans ayrıştırmasında kullanılan değişkenlerde yaşanacak bir değişimin yüzde kaçının kendisinden, yüzde kaçının diğer değişkenlerden meydana geldiğini göstermekte ve değişkenler arasındaki nedensellik ilişkisinin derecesini ortaya çıkarmaktadır. Bir değişkende meydana gelen değişmelerin büyük bir bölümü kendisindeki şoklardan kaynaklanıyorsa bu durum değişkenin dışsal olarak hareket ettiğini göstermektedir (Atay, 2013: 358-359).

İki değişkenli VAR modeli, standart şekilde aşağıdaki şekilde ifade edilmektedir:

$$y_t = a_0 + \sum_{i=1}^{p} a_{1i}\, y_{t-1} + \sum_{i=1}^{p} a_{2i}\, x_{t-i} + v_{1t} \qquad (45)$$

$$x_t = b_0 + \sum_{i=1}^{p} b_{1i}\, y_{t-1} + \sum_{i=1}^{p} b_{2i}\, x_{t-i} + v_{2t} \qquad (46)$$

Denklemde (p) gecikmelerin uzunluğunu gösterirken (v) ortalaması sıfır, kendi gecikmeli değerleriyle olan kovaryansları sıfır ve varyansları sabit, normal dağılıma sahip, rassal hata terimlerini göstermektedir. Tahminin hata varyansı (h) uzunluktaki bir dönem için her bir değişkenin hata varyansına katkısı olarak ifade edilebilmektedir. Daha sonra elde dilen her varyans, toplam varyansa oranlanarak yüzde değeri açısından nispi ağırlığı bulunmaktadır. Ancak varyans ayrışması analizinden elde edilen sonuçların yorumlanması da büyük önem taşımaktadır.45 nolu denklemdeki gibi bir model düşünülürse (v_{1t})'de yaşanacak bir şok, tahmin döneminin uzunluğuna bakılmaksızın x'in öngörü hata varyansını etkilemiyorsa x dışsal olarak kabul edilmektedir. Çünkü böyle bir durumda (x), (y)'den bağımsız hareket etmektedir. Ancak (v_{1t})'de yaşanan bir şok önemli ölçüde (x)'in öngörü hata varyansını etkiliyorsa (x) içsel bir değişken olarak kabul edilmektedir (Aktaş, 2010: 127).

Analiz kapsamında yapılan son analiz ise Granger nedensellik testidir. İstatistiki açıdan nedensellik, bir serinin gelecekte beklenen tahmini değerlerinin, kendisinin veya bağlantılı olduğu zaman serisinin geçmiş dönem değerlerinden etkilenerek elde edilmesidir. Granger nedensellik anlamında ise X değişkeninin başka bir Y değişkenine, hem X hem de Y'deki bilgi veri iken Y değişkeni sadece X değişkenine ait geçmiş değerlerin kullanımıyla tahmin ediliyorsa granger anlamda nedeni olduğu söylenilmektedir. Bir diğer ifadeyle X'in geçmiş değerlerine ait bilgi sahibi olma Y'nin daha keskin bir biçimde tahmin edilmesine olanak sağlıyorsa X değişkeninin Y'nin granger anlamında nedeni olduğu söylenilmektedir (Takım, 2010: 326).

Seriler arasında nedenselliğin test edilebilmesi için durağanlık bilgisine ihtiyaç duyulmaktadır. Seriler arasında eğer eşbütünleşme ilişkisi gözlenmiyorsa serilerin durağan olduğu seviyede nedensellik ilişkisi araştırılabilmektedir. Bu noktada yapısal kırılmalı trend durağan seriler için eşbütünleşme ilişkisinin araştırılması uygun olmayabilmektedir. Dolayısıyla bunun yerine, serilerin kırılma

dönemi dikkate alınarak trendden arındırılması ve daha sonra granger nedensellik testi'nin uygulanması doğru olmaktadır (Büyükakın, Bozkurt ve Cengiz, 2009: 110).

VAR modelinde granger nedensellik analizi yapabilmek için tüm değişkenlerin durağan olması gerekmektedir. Eğer tüm değişkenler durağan ise standart F-testi ile nedensellik ilişkisi test edilmektedir (Barışık ve Kesikoğlu, 2006: 68-69).

Granger nedensellik testi aşağıdaki regresyonun tahmini ile gerçekleşmektedir:

$$Y_t = \alpha_0 + \sum_{i=1}^{n} \beta_i X_{t-i} + \sum_{i=1}^{n} \alpha_i Y_{t-i} + u_i \quad (47)$$

$$X_t = \beta_0 + \sum_{i=1}^{n} \alpha_i x_{t-i} + \sum_{i=1}^{n} \beta_i X_{t-i} + u_i \quad (48)$$

Burada test edilen hipotezler (X)'den (Y)'e doğru nedensellik varsayımı altında,

$$H_0 : \sum \beta_i = 0$$

$$H_1 : \sum \beta_i \neq 0 \quad (49)$$

şeklindedir. Burada (H_0) hipotezi X'ten Y'e granger nedensellik olmadığı varsayımına dayanmaktadır. Alternatifi ise tam tersi granger nedensellik olduğunu ifade etmektedir. Burada klasik işlemlerde hipotezin gerçekleştirilmesi gereken aşamalar bulunmaktadır. İlk adımda kısıtlamasız ilişkideki hata terimleri kareleri toplamının bulunması için,

$$Y_t = \alpha_0 + \sum_{i=1}^{n} \beta_i X_{t-i} + \sum_{i=1}^{n} \alpha_i Y_{t-i} + u_i \quad (50)$$

şeklindeki kısıtlamasız ilişki tahmin edilerek hata terimleri kareleri toplamı $\sum_{t=1}^{n} e_1^2$ bulunmaktadır. Buda RSS_{UR} olarak gösterilmektedir. İkinci adımda kısıtlı ilişkideki hata terimleri kareleri toplamının bulunması için $\sum_{i=1}^{n} \beta_i X_{t-i}$ terimi dışarıda tutulmaktadır. Geride kalan,

$$Y_t = \alpha_0 + \sum_{i=1}^{n} \alpha_i Y_{t-i} + u_i \quad (51)$$

İlişkisi tahmin edilerek, bu kısıtlamalı ilişkinin hata terimleri kareleri toplamı $\sum_{r=1}^{n} e_1^2$ olarak bulunmaktadır. Bu ise RSS_R olarak ifade edilmektedir.

Hipotezin testinde aşağıdaki F değeri hesaplanmaktadır (Tarı, 2015: 438-439):

$$F = \frac{(RSS_R - RSS_{UR})/m}{RSS_{UR}/(n-k)} \quad (52)$$

Burada (RSS_R) kısıtlamalı ilişkideki hata terimlerinin kareleri toplamını, (RSS_{UR}) kısıtlamasız ilişkideki hata terimlerinin kareleri toplamını, (m) dışarıda bırakılan gecikmeli değişken sayısını, (n) örnek hacmi ve son olarak (k) ise kısıtlamasız regresyonda tahmin edilen parametre sayısını göstermektedir. Burada daha sonra hesaplanan F değeri F tablosundan $F_a(m, n-k)$ değeri bulunmakta ve karşılaştırılarak karar verilmektedir. Eğer hesaplanan F değeri F tablo değerinden küçük ise X değişkeninden Y değişkenine doğru nedensellik olmadığı kabul edilmektedir. Ancak tam tersi hesaplanan F değeri F tablo değerinden büyük ise hipotez reddedilerek alternatifi kabul edilmekte ve değişkenler arasında nedensellik ilişkisi olduğu sonucuna ulaşılmaktadır.

3. 2. 2. Kripto Para ve Döviz Kuru İlişkisine Yönelik Analiz

Çalışmanın bu bölümünde kripto para Bitcoin ile döviz kuru arasındaki ilişki analiz edilmiş ve analizden elde edilen sonuçlar verilmiştir.

3. 2. 2. 1. Analizde Kullanılan Veri Seti

Kripto paraların son zamanlarda giderek yaygınlaşmasıyla birlikte bu para birimlerinin dünya ekonomisi üzerinde olumlu ya da olumsuz ne tür bir etki yaratacağı düşünülmeye başlanmıştır. Çalışmada da temel ve en popüler kripto para birimi olan Bitcoin (BTC)'in majör döviz birimleri olarak da bilinen ve dünya borsalarında en çok işlem gören para birimlerinden olan Euro (EUR), İngiliz Sterlini (GBP), Avustralya Doları (AUD), Japon Yeni (JPY), Kanada Doları (CAD), İsviçre Frangı (CHF) ve Çin Yuanı (CNY) arasındaki ilişki analiz edilerek bu konuya aydınlık kazandırılmaya çalışmıştır. Analize dâhil edilen para birimlerinin, tüm dünya üzerinde en çok kabul gören para biriminin Amerikan Doları (USD) olması nedeniyle, USD karşısındaki çapraz kur verilerinden yararlanılmıştır.

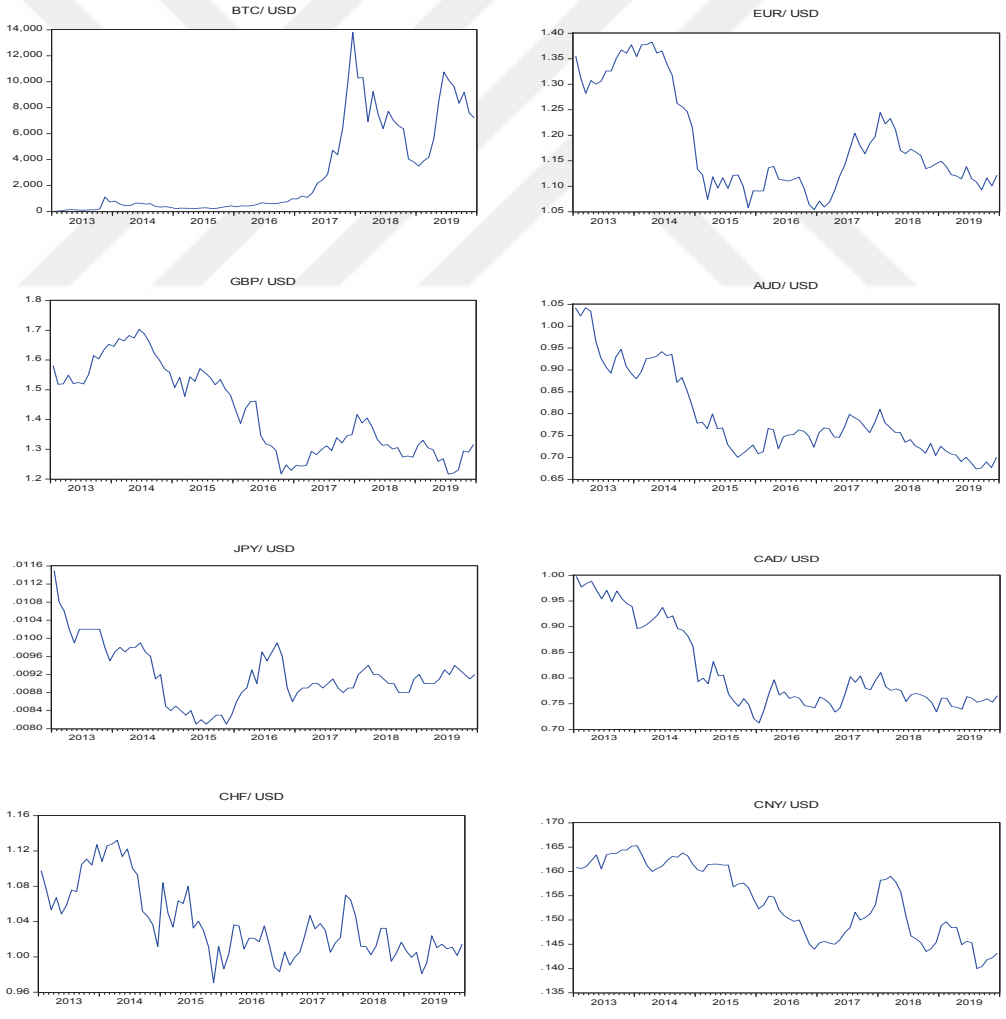
Bitcoin'in piyasada işlem gören en yeni para birimlerinden biri olmasının etkisiyle veriler 2013 yılından başlatılmış ve 2013-2019 dönemine ait aylık veriler kullanılarak gözlem sayısı 84 ile sınırlandırılmıştır. Bu veriler ise Türkiye Cumhuriyeti Merkez Bankası verilerinden elde edilirken aynı zamanda bu verilerin toplanmasında "investing.com" ve "yahoo finans" adreslerinden yararlanılmıştır. Değişkenler içerisinden Bitcoin, bağımlı değişken olarak ele alınmış ve çalışmada BTC/USD olarak gösterilmiştir. Diğer para birimleri ise EUR/USD, GBP/USD, AUD/USD, JPY/USD, CAD/USD, CHF/USD ve son olarak CNY/USD olarak gösterilmiştir. Bu değişkenler de çalışmada bağımsız değişken olarak yer almış ve analiz gerçekleştirilmiştir.

Çalışmada yapılan ARDL analizi sonucunda değişkenler arasında uzun dönemli bir ilişki tespit edilememiştir. Bu sebepten dolayı da değişkenler arasındaki kısa dönemli ilişkiyi analiz edebilmek için VAR analizi uygulanmıştır. Ancak VAR analizinin uygulanabilmesi için de tüm değişkenlerin seviyede durağan olması gerekmektedir. Bundan dolayı bu değişkenlerden seviyede durağan olmayanların farkları alınarak seviyede durağan hale getirilmiştir. Durağan hale getirilen

değişkenler ise çalışmada DBTC/USD, DEUR/USD, DGBP/USD, DAUD/USD, DJPY/USD, DCAD/USD, ve DCNY/USD olarak gösterilmiştir. Tüm bu işlemlerin yapılıp analizin gerçekleştirilmesinde ise EViews 9 programından yararlanılmıştır.

3. 2. 2. 2. Değişkenlerin Başlangıç Terimi ve Trend Durumu

Çalışmada analizi gerçekleştirebilmek amacıyla birim kök testinin yapılması gerekmektedir. Ancak değişkenlerin durağan olduğu seviyeyi belirlemek için birim kök testi yapılmadan önce tüm değişkenlerin grafikleri doğrultusunda trend ve regresyon sabitini ifade eden başlangıç teriminin olup olmadığının incelenmesi gerekmektedir.



Şekil 29: Değişkenlerin Başlangıç Terimi ve Trend Durumları

Şekil 29'a bakıldığı zaman tüm değişkenlerin aşağı ve yukarı yönlü sürekli bir dalgalanma gösterdiği dolayısıyla tüm değişkenlerin trend içerdiği görülmektedir. Ayrıca volatilitesindeki dalgalanmalarla sürekli dikkat çeken Bitcoin'in grafiğine bakıldığı zaman eğrinin keskin bir iniş ve çıkış eğilimi sergilediği görülmektedir. Bu durum literatürde de belirtildiği üzere Bitcoin'in diğer para birimleri karşısında keskin bir dalgalanma özelliği gösterdiğini doğrulamaktadır. Diğer yandan majör para birimlerinin hiçbirinin sıfır noktasından başlamadığı da Şekil 29'dan anlaşılmaktadır. Bitcoin'in ise sıfır noktasına çok yakın bir değerde başlamasına karşın tam sıfır noktasında olmadığı görülmektedir. Bu durumun ise Bitcoin'in 2009 yılında ortaya çıkmasıyla birlikte 2013 yılında fiyatlarının oluşmaya başlamasıyla ilgili olduğu bilinmektedir. Bu genel değerlendirmeyle birlikte değişkenlerin hiçbiri tam sıfır noktasından başlamadığı için hepsinin başlangıç terimi içerdiği sonucuna ulaşılmıştır.

3. 2. 2. 2. Birim Kök Testi Sonuçları

Değişkenler arasındaki ilişkinin en doğru şekilde test edilebilmesi için tüm değişkenlere birim kök testi uygulanarak durağan olduğu seviyenin tespit edilmesi gerekmektedir. Bu kapsamda yapılabilen birçok birim kök testi olmasına karşın çalışmada iki farklı birim kök testinden yararlanılmıştır. Öncelikli olarak Augmented Dickey-Fuller (ADF) testi yapılarak değişkenler incelenmiştir. ADF birim kök testi sonuçları Tablo 15'de gösterilmiştir.

Tablo 15: ADF Birim Kök Testi Sonuçları

Değişkenler	Düzeyde		Birinci Farkında	
	ADF Değerleri	Olasılık Değerleri	ADF Değerleri	Olasılık Değerleri
BTC/USD	2,348	0,403	8,627	0,000
EUR/USD	1,452	0,837	8,568	0,000
GBP/USD	1,814	0,689	5,187	0,000
AUD/USD	2,438	0,357	8,631	0,000
JPY/USD	3,283	0,076	9,087	0,000
CAD/USD	1,786	0,702	6,501	0,000
CHF/USD	3,488	0,047	-	-
CNY/USD	2,908	0,165	6,882	0,000
ADF birim kök testi için kritik değerler MacKinnon (1996)'dan elde edilmiştir.				

Tablo 15'e bakıldığı zaman tüm değişkenler önce seviyede daha sonra da birinci farklarında durağanlık testine tâbi tutulmuştur. ADF testine göre %5 anlamlılık düzeyinde CHF/USD değişkeni seviyede durağan bulunurken diğer tüm değişkenler birinci farklarında durağan bulunmuştur. Bunun anlamı CHF/USD değişkeni I(0) iken diğer değişkenler I(1)'dir. Çalışmada ADF testinin sonuçlarının doğruluğunun onaylanması için ayrıca Philips-Perron (PP) birim kök testi yapılmış ve bu testin sonuçlarına Tablo 16'da yer verilmiştir.

Tablo 16: PP Birim Kök Testi Sonuçları

Değişkenler	Düzeyde		Birinci Farkında	
	PP Değerleri	Olasılık Değerleri	PP Değerleri	Olasılık Değerleri
BTC/USD	2,433	0,360	8,625	0,000
EUR/USD	1,642	0,7676	8,593	0,000
GBP/USD	1,769	0,710	9,899	0,000
AUD/USD	2,399	0,3772	8,621	0,000
JPY/USD	3,298	0,073	9,087	0,000
CAD/USD	1,597	0,785	9,337	0,000
CHF/USD	3,495	0,046	-	-
CNY/USD	2,638	0,264	6,885	0,000
PP birim kök testi için kritik değerler MacKinnon (1996)'dan elde edilmiştir. PP testi değişkenlerin durağan olduğu seviyeyi test ederken hipotezde birim kökün olduğunu alternatif hipotezde ise birim kök olmadığını ifade etmektedir.				

PP testi sonuçları da CHF/USD değişkeninin seviyede diğer değişkenlerin ise birinci farkında olduğu sonuçlarını vermiştir. Bu sonuçlar ADF birim kök testi sonuçları doğrulamıştır. Elde edilen tüm bu sonuçlar doğrultusunda CHF/USD değişkeninin I(0) diğer değişkenlerin I(1) olduğu anlaşılmıştır. Bu durum değişkenlerin farklı seviyede durağan olduğu zamanlarda değişkenler arasında ilişkiyi analiz etmeye olanak sağlayan ARDL analizinin yapılması gerektirmektedir. Dolayısıyla çalışmanın sonraki kısmında ARDL analizi yapılıp değişkenler arasında uzun ve kısa dönemli ilişki olup olmadığı analiz edilmiştir.

3. 2. 2. 3. ARDL Analizi Sonuçları

ARDL (Autoregressive Distributed Lag) analizi farklı seviyelerde değişkenlerin analiz edilmesine olanak sağlayan bir analizdir. ARDL analizinde

değişkenler arasındaki uzun ve kısa dönemli ilişkinin analiz edilebilmesi için öncelikli olarak uygun gecikme uzunluğunun belirlenmesi ve analize bu doğrultuda devam edilmesi gerekmektedir. Tablo 17'de ARDL analizi izin uygun gecikme uzunlukları verilmiştir.

Tablo 17: ARDL Analizi İçin Uygun Gecikme Uzunluğu

Gecikme Sayısı	LR	FPE	AIC	SC	HQ
0	NA	2,760	22,332	22,087	22,234
1	824,077*	6,840	32,947	30,739*	32,065
2	57,718	1,460	32,242	28,071	30,575
3	73,345	2,150	31,995	25,862	29,544
4	59,902	3,850	31,704	23,608	28,469
5	56,908	6,930	31,646	21,587	27,626
6	59,168	1,050	32,153	20,132	27,349
7	77,325	4,890	34,539	20,554	28,950
8	76,104	6,110*	39,773*	23,826	33,400*

Literatür ayrıntılı bir şekilde incelendiğinde (Dirican ve Canöz, 2017; Yıldırım, 2013 ve Yıldız, 2018)'de olduğu gibi uygun gecikme uzunluğunun belirlenmesi için daha çok AIC ve SC kriter değerlerinden yararlanıldığı görülmektedir. Tablo 17'ye bakıldığı zaman hem en yaygın kullanılan kriter değerlerinden biri olan AIC değeri hem de FPE ve HQ değerleri analiz için en uygun gecikme uzunluğunun 8 olduğunu göstermektedir. Dolayısıyla çalışmada uygun gecikme uzunluğu 8 olarak alınarak ARDL analizi gerçekleştirilmiştir. ARDL analizi kapsamında ise ilk olarak değişkenler arasında uzun dönemli ilişki olup olmadığını anlayabilmek için sınır testi yapılmış ve elde edilen sonuçlar Tablo 18'de gösterilmiştir.

Tablo 18: Sınır Testi Sonuçları

K	F-istatistik	Alt Sınır I(0)	Üst Sınır I(1)
7	2,127	2,32	3,5
* K bağımsız değişken sayısını göstermektedir. ** H0: Uzun dönemli ilişki yok H1: Uzun dönemli ilişki var *** % 5 anlamlılık düzeyinde değerlendirilmiştir.			

Sınır testi elde edilen F istatistik değerinin alt ve üst sınır bant değerleri açısından yorumlanmaktadır. Burada eğer F-istatistik değeri üst sınır değerinin üzerindeyse H0 hipotezi reddedilirken alternatif hipotez kabul edilmektedir. Tam tersi F-istatistik değeri alt sınır değerinin altındaysa H0 hipotezi kabul edilerek değişkenler arasında uzun dönemli ilişki olmadığı sonucuna ulaşılmaktadır. Ancak elde edilen F-istatistik değerleri alt ve üst sınır arasında bir değerde alabilmektedir. Böyle bir durumda eşbütünleşmenin varlığıyla ilgili herhangi bir yorum yapılamamaktadır. Çalışmada yapılan analiz sonucuna bakıldığı zaman F-istatistik değerinin alt sınır değerinden daha düşük olduğu görülmektedir. Bu durumda H0 hipotezi kabul edilirken kripto para Bitcoin ve döviz kurları arasında uzun dönemli bir ilişki olmadığı sonucuna ulaşılmıştır. Bundan dolayı değişkenler arasındaki ilişkiyi ayrıntılı bir şekilde görebilmek için çalışmaya VAR analizi ile devam edilmiştir.

3. 2. 2. 4. VAR Analizi Sonuçları

Vektör Otoregresyon Modeli (VAR) kısa dönemli bir analiz olup analizin yapılabilmesi için tüm değişkenlerin seviyede durağan olması gerekmektedir. Bundan dolayı çalışmada analizi gerçekleştirmek için I(1) olan değişkenlerin farkları alınarak seviyede durağan hale getirilmiştir. Farkları alındıktan sonra ise değişkenler DBTC/USD, DEUR/USD, DGBP/USD, DAUD/USD, DJPY/USD, DCAD/USD, ve DCNY/USD olarak gösterilmiştir. Daha sonra uygun gecikme uzunluğu tespit edilmiş ve elde edilen sonuçlar Tablo 19'da gösterilmiştir.

Tablo 19: VAR Analizi İçin Uygun Gecikme Uzunluğu

Gecikeme Sayısı	LR	FPE	AIC	SC	HQ
0	NA	3,460	31,316	31,069*	31,218
1	169,088*	1,490*	32,172	29,947	31,283*
2	71,867	2,510	31,704	27,502	30,026
3	42,386	6,860	30,845	24,665	28,377
4	66,379	1,050	30,719	22,561	27,462
5	44,948	2,700	30,334	20,199	26,287
6	62,198	3,600	31,020	18,907	26,183
7	61,857	3,620	32,750	18,659	27,124
8	59,216	1,710	36,965*	20,897	30,549

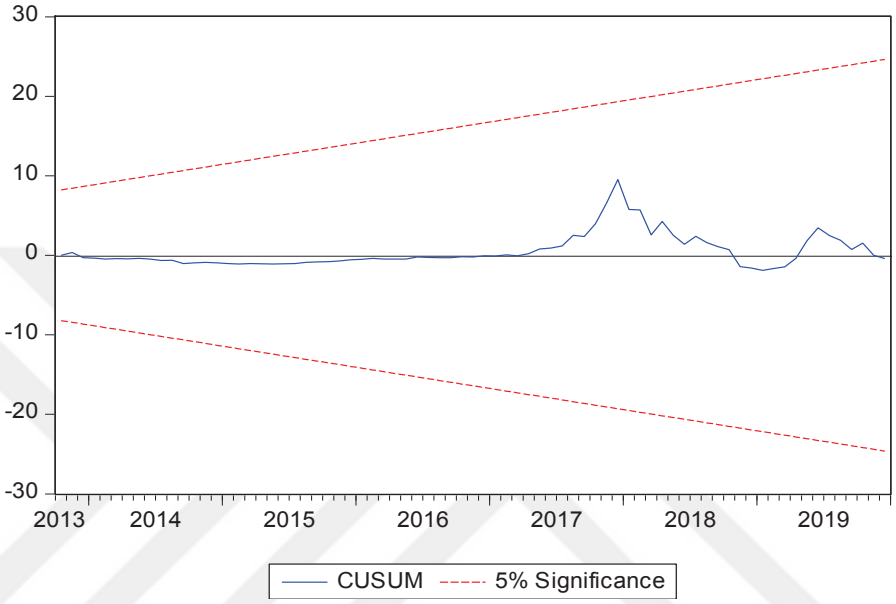
Tablo 19'da VAR analiz için uygun gecikme uzunlukları gösterilmiştir. Literatür kapsamında en çok kabul edilen kriterin AIC ve SC olmasına karşın analizde her iki kriterde, gecikme sayısını birbirinden ve diğer kriterlerden farklı vermiştir. Bundan dolayı analizde çoğunluğun gecikme uzunluk sayısını 1 vermesi dikkate alınmış ve gecikme uzunluğu 1 olarak ele alınarak VAR analizi gerçekleştirilmiştir. Analiz sonrasında elde edilen istatistiki değerler ise Tablo 20'de verilmiştir.

Tablo 20: VAR Analizi İstatistik Değerleri

	R-Kare	Düz R-Kare	Hata Kareleri Toplamı	Standart Hata
DBTC/USD	0,039	-0,066	95844	1145,83
DEUR/USD	0,079	-0,021	0,041	0,023
DGBP/USD	0,110	0,013	0,078	0,032
DAUD/USD	0,100	0,001	0,036	0,022
DJPY/USD	0,121	0,025	3,560	0,000
DCAD/USD	0,101	0,003	0,024	0,018
CHF/USD	0,754	0,728	0,031	0,020
DCNY/USD	0,179	0,089	0,000	0,001
	F-istatistiği	Log Olabilirlik	Akaike AIC	Schwarz SC
DBTC/USD	0,372	-689,185	17,028	17,293
DEUR/USD	0,788	194,762	-4,530	-4,266
DGBP/USD	1,133	168,833	-3,898	-3,634
DAUD/USD	1,015	200,038	-4,659	-4,395
DJPY/USD	1,261	578,733	-13,895	-13,631
DCAD/USD	1,034	216,091	-5,051	-4,786
CHF/USD	28,100	205,631	-4,795	-4,531
DCNY/USD	1,994	411,390	-9,814	-9,550
Det. Kalıntı Kov.		2,780		
Log Olabilirlik		1387,436		
AIC		-32,083		
SC		-29,970		

VAR analizi istatistik değerleri gözlemlendikten sonra verilerin güvenli bant aralığında kalıp kalmadığı da incelenerek yapısal kırılma durumlarının değerlendirilmesi de önem arz etmektedir. Bu analiz CUSUM testi ile yapılırken,

güvenli bant aralığındaki yerinin net bir şekilde anlaşılabilmesi için grafikle gösterilmesi uygun görülmektedir. Bu doğrultuda yapılan CUSUM testi grafiği Şekil 30'da görülmektedir.



Şekil 30: CUSUM Test Sonucu

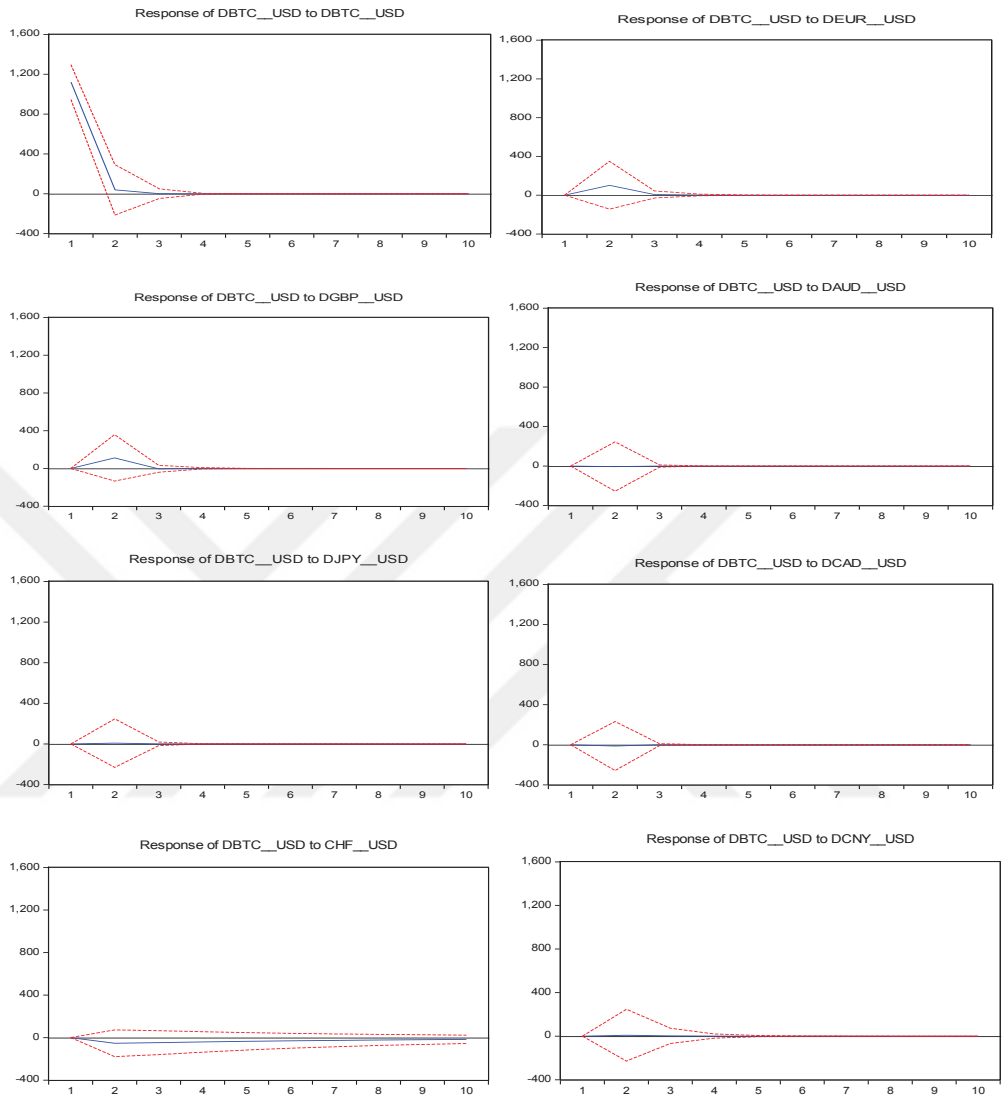
Şekil 30'a bakıldığı zaman veri setinin güvenli bir bant aralığında yer aldığı net bir şekilde görülmektedir. Bu şekilde bir sapma olmaması veri setinde yapısal bir istikrarın olduğunu göstermektedir. CUSUM testiyle gerçekleştirilen analiz sonucunda değişkenler üzerine verilen bir şok karşısında hangi bağımsız değişkenin bağımlı değişkeni daha fazla etkilediğine yani şokların etkisinin neyden kaynaklandığını analiz edilecektir. Bunun için gerekli olan analiz ise varyans ayrıştırmasıdır. Ayrıca değişkenlerin içsel bir değişken mi yoksa dışsal bir değişken mi olduğunun anlaşılması da önemlidir. Dolayısıyla varyans ayrıştırması analizi sayesinde değişkenin içsel bir değişken mi yoksa dışsal bir değişken mi olduğu anlaşılacaktır. Bu analizin sonuçları ise Tablo 21'de gösterilmiştir.

Tablo 21: Varyans Ayrıştırması Sonuçları

DÖNEM	1	2	3	4	5	6	7	8	9	10
S.E.	1145,8	1160,3	1162,7	1164,1	1165,1	1165,8	1166,4	1166,8	1167,2	1167,4
DBTC/USD	100,00	97,57	97,167	96,939	96,779	96,658	96,565	96,495	96,443	96,404
DEUR/USD	0,00	0,55	0,582	0,613	0,646	0,671	0,693	0,709	0,722	0,731
DGBP/USD	0,00	0,565	0,567	0,570	0,570	0,569	0,569	0,568	0,568	0,568
DAUD/USD	0,00	0,525	0,536	0,540	0,539	0,539	0,538	0,538	0,538	0,538
DJPY/USD	0,00	0,029	0,048	0,055	0,063	0,071	0,076	0,080	0,083	0,086
DCAD/USD	0,00	0,448	0,446	0,474	0,483	0,489	0,493	0,497	0,499	0,501
CHF/USD	0,00	0,307	0,527	0,677	0,788	0,872	0,934	0,981	1,015	1,040
DCNY/USD	0,00	0,002	0,123	0,127	0,127	0,127	0,127	0,127	0,127	0,127

Tablo 21'de varyans ayrıştırması sonuçlarını göstermektedir. Tablo 21'den görülen sonuçlara göre Bitcoin'in birinci dönemde sadece kendi şokları tarafından belirlendiği ve yine tüm dönem içerisinde en çok kendi gecikmelerinden etkilediği sonucuna ulaşılmıştır. 10 dönemin sonunda bağımlı değişken olan Bitcoin'in kendi gecikmelerinden %96 oranında etkilenirken diğer değişkenlerden ortalama olarak aynı düzeyde etkilenmektedir. Sırasıyla İsviçre Frangı, Euro, İngiliz Sterlini, Avustralya Doları, Kanada Doları, Çin Yuanı ve Japon Yeni'nden %1,04, %0,73, %0,56,%0,53, %0,50, %0,12 ve %0,08 oranlarında etkide bulunmaktadırlar. Varyans ayrıştırması analizinden bu elde edilen tüm bu sonuçlar kripto para Bitcoin'in dışsal bir değişken olduğunu göstermektedir. Yani çalışma kapsamında bağımlı değişken olarak ele alınan Bitcoin'in dışsal olarak hareket ettiği anlaşılmıştır.

Bu analizle birlikte çalışmada bir sonraki aşamada değişkenler arasındaki etki-tepki ilişkisi analiz edilmektedir. Yani bir bağımsız değişkene verilen bir şokun diğer değişkene etkisi incelenmektedir. Etki-tepki analizi sonuçları Şekil 31'de gösterilmiştir.



Şekil 31: Etki-Tepki Analizi Sonuçları

Etki-Tepki Analizi ile birlikte değişkenlerde meydana gelen bir standart hata kadarlık şoklar karşısında diğer değişkenlerin gösterdiği dinamik tepkiler incelenmektedir. Şekil 31'de tüm değişkenlere verilen bir şokun BTC üzerindeki etkisini göstermektedir. Şekilde düz çizgiler nokta tahminlerini kesikli çizgiler de bir standart hatalık güven sınırlarını göstermektedir. Bu doğrultuda Şekil 31'e bakıldığı zaman genel eğilimin tüm değişkenler için üçüncü dönemde dengeye yakınsadığı ve bu dönemde sonra BTC'nin kendi ortalamasına yöneldiği net bir şekilde görülmektedir. Farklı olarak CHF'ye verilen bir birimlik şokun BTC üzerindeki

etkisine bakıldığı zaman BTC'nin hiçbir zaman kendi dengesine tam anlamıyla yönelmediği çünkü her durumda kendi ortalamasına yaklaşmakla birlikte belli bir dönem sonunda tam dengeye gelmeden sabit bir çizgi şeklini aldığı görülmektedir. Etki-Tepki analizinden sonra çalışma kapsamında son olarak değişkenlerin birbirlerini çift ve tek yönlü etkileme durumunu görebilmek amacıyla granger nedensellik testi yapılmış ve sonuçlar Tablo 22'de gösterilmiştir.

Tablo 22: Granger Nedensellik Testi Sonuçları

	Olasılık Değerleri	Sonuç	Nedensellik
DEUR/USD ⇨ DBTC/USD	0,408	Kabul	Yok
DBTC/USD ⇨ DEUR/USD	0,187	Kabul	Yok
DGBP/USD ⇨ DBTC/USD	0,366	Kabul	Yok
DBTC/USD ⇨ DGBP/USD	0,397	Kabul	Yok
DAUD/USD ⇨ DBTC/USD	0,963	Kabul	Yok
DBTC/USD ⇨ DAUD/USD	0,121	Kabul	Yok
DJPY/USD ⇨ DBTC/USD	0,948	Kabul	Yok
DBTC/USD ⇨ DJPY/USD	0,599	Kabul	Yok
DCAD/USD ⇨ DBTC/USD	0,914	Kabul	Yok
DBTC/USD ⇨ DCAD/USD	0,033	Red	Var
CHF/USD ⇨ DBTC/USD	0,398	Kabul	Yok
DBTC/USD ⇨ CHF/USD	0,041	Red	Var
DCNY/USD ⇨ DBTC/USD	0,941	Kabul	Yok
DBTC/USD ⇨ DCNY/USD	0,034	Red	Var
Tablo'da nedenselliğin olmadığı hipotezi altında ok yönü analiz edilen değişkenin yönünü göstermektedir.			

Tablo 22'de bağımlı değişken Bitcoin ile bağımsız değişken olan majör para birimleri arasındaki nedensellik ilişkisi açıkça görülmektedir. Yapılan analiz sonucunda Bitcoin'den Kanada Dolarına doğru %5 anlamlılık düzeyinde tek yönlü bir nedensellik ilişkisi olduğu sonucuna ulaşılmıştır. Ayrıca yine %5 anlamlılık düzeyinde Bitcoin'den İsviçre Frangı'na ve Çin Yuanı'na doğru tek yönlü bir nedensellik ilişkisi saptanırken diğer bağımsız değişkenlerle Bitcoin arasında bir granger nedensellik ilişkisi saptanamamıştır.

SONUÇ

Piyasada son zamanlarda en popüler olan ve en çok tartışılan para birimleri kripto paralardır. Kripto paralar 2008 yılının sonunda Bitcoin'in tanıtılmasıyla birlikte gündeme gelmeye başlamış zaman geçtikçe de insanların, devletlerin ve yatırım şirketlerinin ilgisini daha çok çekmeyi başarmıştır. Ancak bu kadar kısa bir zaman önce adını duyurmuş bir para birimi olmasına rağmen hakkında bu kadar çok konuşulması, bu para birimlerinin bir balon mu olup olmadığı gibi soruları gündeme getirmiştir. Ayrıca bu sanal para birimlerinin volatilitesindeki yükseklikte soru işaretlerini daha çok tetiklemiş ve bu para birimleri ekonomistlerin de ilgisini çekmeyi başarmıştır. Bu doğrultuda kripto paralarla ilgili literatürde birçok araştırma yapılmış olsa bile, merkezi para birimlerinden farklılık sergilemesinin etkisiyle, kripto paralar insanların aklında hâlâ büyük bir soru işareti olarak kalmış ve konunun her yönüyle ayrıntılı bir şekilde açıklanmasını zorunlu hale getirmiştir.

Kripto paralar matematiksel kriptoloji yöntemleriyle güvenliği sağlayan, merkezi olmayan ve eşler arası bir sisteme dayanan sanal para birimleri olarak tanımlanmaktadır. Güvenlik açısından bu kadar önemli bir yere sahip olan kriptoloji ise bir şifreleme bilimi olup verilerin belirli bir sisteme göre şifrelenerek güvenli bir ortam oluşturulması, verinin alıcıya gönderilmesi ve bu şifreleme sisteminin çözülmesi yoluyla da verilerin ortaya çıkarılması süreci olarak açıklanmaktadır. Bu doğrultuda kripto paralar çift anahtarlı şifreleme yöntemine dayanan asimetrik şifreleme yöntemini kullanmakta ve bu şekilde güvenliğini sağlamaktadır. Kısacası Altın gibi değerli madenlerin bulunması için belirli kazılar yapılması gerektiği gibi kripto paraları bulmak ve bunları kullanmak için de çeşitli matematiksel problemlerin farklı yazılımlar aracılığıyla çözülmesi gerekmektedir. Ancak şifreli korumaya karşın kripto paralar merkezi bir otoriteye bağlı olmayıp herhangi bir hükümet tarafından üretilmezler ve bir denetlemeye de tabi değillerdir. Bu paraların üretimi ve kullanımı tamamen kullanıcı temelli olup üretimleri sınırlandırılmıştır. Ayrıca çok küçük parçalara bile bölünebilmektedirler. Kripto paranın bu özelliği ise literatürde bu paraların ilgi çekmesindeki en önemli nedenlerden biri olarak gösterilmektedir.

Kripto paranın sahip olduğu bunun gibi çeşitli özellikleri ve özellikle de klasik para birimlerinden farklı özellikler sergilemesi ise ayrıca bu para birimlerinin ekonomik yönden nasıl bir etkisi olacağı sorularını da gündeme getirmiştir. Çalışmada bu konunun bir kısmına açıklık kazandırmak amacıyla kripto paralar ve temel para birimleri arasındaki ilişki analiz edilmeye çalışılmıştır. Bu doğrultuda Bitcoin bağımlı değişken olarak ele alınırken piyasada en çok işlem gören para birimleri bağımsız değişken olarak ele alınmış ve değişkenlerin çapraz kur verilerinden yararlanılmıştır. Analiz kapsamında öncelikli olarak eşbütünleşme analizi ve akabinde VAR analizi yapılmıştır. Bitcoin ile temel para birimleri arasındaki eşbütünleme ilişkisi ARDL analizi ile sınanmış ve aralarında uzun dönemli bir ilişki saptanamamıştır. Ayrıca yapılan varyans ayrıştırması sonuçları da Bitcoin'in dışsal bir değişken olduğunu ortaya koymuştur. Çalışma da ayrıca değişkenler arasında uzun dönemli bir ilişki çıkmamasının etkisiyle değişkenlerin birbirlerini nasıl etkilediğini anlayabilmek için granger nedensellik testi yapılmıştır. Yapılan nedensellik testi sonuçları ise Bitcoin'den İsviçre Frangı'na ve Çin Yuanı'na doğru tek yönlü bir nedensellik olduğunu ortaya koyarken diğer değişkenler arasında nedensellik bulgusuna rastlanılamamıştır.

Literatürde bunun gibi kripto paralara yönelik daha birçok çalışma ve varsayımlar olup bu konuya ilişkin bilgi yetersizlikleri biraz daha azaltılmaya çalışılmaktadır. Zaman içerisinde belirsizlikler ortadan kalktıkça kripto paralara olan ilginin bu süreçle birlikte artıp azalacağı yönünden net bir çıkarımda bulunulamamaktadır. Ancak kripto para birimlerinin zaman içerisinde tanınmaya başlanması ve özelliklerinin anlaşılmasıyla birlikte ABD, Avustralya, Birleşik Krallık, Estonya, Güney Kore, Hollanda, İzlanda, İsveç, İsviçre, Japonya, Meksika ve Kanada gibi bazı ülkelerde yasal hale getirilmeye başlanması ve bu yasallaşmanın ülkeler arasında giderek yaygınlaşması kripto para birimlerinin giderek para piyasalarında daha çok yer bulmaya başlayacağının göstergesidir. Üstelik Türkiye'de dahil olmak üzere Almanya, Belçika, Çin, Danimarka, Fransa, Rusya, Venezuela ve Yunanistan gibi bazı ülkelerin de kripto parayı tam anlamıyla yasal bir para birimi olarak kabul etmese bile ülke içerisinde kullanımının, özellikle yatırım yapmayı planlayanların fazlasıyla ilgisini çekmesinin etkisiyle, engellenememesi de Bitcoin başta olmak üzere birçok kripto paranın zaman içerisinde daha da yaygın kullanılmaya başlanılacağını göstermektedir.

Ülkelerin kripto paraları yasal ve yasa dışı kabul etmesinin yanı sıra şifreli para birimlerinin her ülke tarafından emtia, menkul kıymet ya da para olarak ayrı ayrı değerlendirip farklı sonuçlara ulaşılmasına neden olmuştur. Bu doğrultu da ise ABD, Kanada ve Japonya gibi ülkeler kripto parayı emtia olarak nitelendirken Almanya ve Hollanda gibi ülkelerde ise diğer para birimleri gibi bir para olarak değerlendirmiş ve bu doğrultuda kripto para birimlerini vergilendirmeye yönelik çalışmalar yapmaya başlamışlardır. Ülkelerin bu şekilde kripto paraları vergilendirmeye yönelik çalışmalar yapmaları da kripto paraların etkinliğinin artacağının bir göstergesi niteliğinde değerlendirilmektedir.

Çalışma kapsamında bu doğrultuda yapılacak öneri, kripto paralarla yapılacak her türlü işlemlerde ve yatırımlarda konu hakkında tam ve net bir bilgiye sahip olunmadan hareket edilmemesidir. Bu kapsamda yapılması önerilen şey ise konuyla ilgili araştırmalar yapılarak bilgi yetersizliklerinin ortadan kaldırılmasıdır. Ancak bu şekilde gerek bireyler açısından gerek ülke ekonomileri açısında en doğru kararlar alınacak ve maksimum fayda elde edilmiş olunacaktır. Dolayısıyla bundan sonra bu konuda yapılacak çalışmalarda kripto paraların farklı bir yönü analiz edilirken mevcut analizlere de farklı bir bakış açısıyla yaklaşılması da önem taşımaktadır. Özellikle de yapılacak sonraki çalışmalarda kripto para birimlerinin merkezi yönetimden bağımsız olmasının etkisiyle merkez bankacılığına olan etkisinin incelenmesi ve bunun yanı sıra finansal hizmetler ile dış ticaret işlemleri üzerinde yaratacağı etkilerin de ayrıca bakılıp incelenmesi literatüre önemli kazanımlar sağlayacağı düşünülmektedir.

KAYNAKÇA

Aba Şenbayram, E. (2019). Paranın Geldiği Uç Nokta: Bitcoin. *Econharran Harran Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 3(4), 72-92.

Abaday, A. (2018). *Nasıl Bitcoin Zengini Olunur?*.(1. Basım). İstanbul: Madrabaz Kitap.

Adana Karaağaç, G. ve Altınırmak, S. (2018). En Yüksek Piyasa Değerine Sahip On Kripto Paranın Birbirleriyle Etkileşimi. *Muhasebe ve Finansman Dergisi,* 79, 123-128.

Adıgüzel, U. (2012). *Para Politikasının Türkiye Ekonomisi Üzerindeki Etkilerinin VAR yöntemleri ile Ölçülmesi.* Yayımlanmamış Doktora Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.

Agrawal, M. and Mishra, P. (2012). A Comparative Survey on Symmetric Key Encryption Techniques. *International Journal on Computer Science and Engineering (IJCSE),* 4(5), 877-882.

Ahamad, S., Nair, M. and Varghese, B. (2013). *A Survey on Crypto Currencies.* Paper presented at the 4th International Conference on Advances in Computer Science.

Ahmed, M., Sanjabi, B., Aldiaz, D., Rezaei, A. and Omotunde, H. (2012). Diffie-Hellman and Its Application in Security Protocols. *International Journal of Engineering Science and Innovative Technology (IJESIT),* 1(2), 69-73.

Akben, S. B. ve Subaşı, A. (2005). RSA ve Eliptik Eğri Algoritmasının Performans Karşılaştırması. *KSU FEN ve Mühendislik Dergisi,* 8(1). 35-40.

Akcan, A. T. (2018). Türk Borsalarında İşlem Gören Seçilmiş Kripto Paralar., Alptekin, V., Metin, İ. ve Akcan, A. T. (Editörler). *Kripto Para Ekonomisi.* Birinci Baskı. Konya. Eğitim Yayınevi, ss.137-158.

Akçeşme, D. ve Sönmez, A. Ç. (2008, 16-18 Mayıs). *Bir Sanal Noter Uygulamasının Gerektirdikleri.* Ağ ve Bilgi Güvenliği Sempozyumunda sunuldu, Girne, KKTC.

Akıl, A. (2019). *Euro/Dolar Paritesindeki Değişimin Zaman Serisi Analizi ile İncelenmesi.* Yayımlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta.

Akiz, E. H. (2019). *Kripto Paranın Vergilendirilmesi, Muhasebeleştirilmesi ve Denetimi,* Tartışma Metni, İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü, İstanbul.

Aksoy, E. E. (2018). *Bitcoin Paradan Sonraki En Büyük İcat Blockchain Teknolojisi ve Altcoin'ler.* (1.Baskı). İstanbul: Abaküs Yayınları.

Aktaş, C. (2010). Türkiye'de Reel Döviz Kuru ile İhracat ve İthalat Arasındaki İlişkinin VAR Tekniğiyle Analizi. *Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Dergisi,* 6(11), 123-140.

Aktaş, G. (2018). Akıllı Sınır Yaklaşımı Çerçevesinde Blok Zinciri Teknolojisinin Gümrük İşlemlerinde Potansiyel Kullanım Alanları. *Gümrük Ticaret Dergisi,* 5(14), 18-31.

Alajbegović, H., Jamak, H. and Zečić, D. (2006, 11-15 Sempember). Paper presented at *Digital Signature Algorithm (DSA).* 10th International Research/ Expert Conference "Trends in Development of Machinery and Associated Technology", Barcelona-Lloret de Mar, Spain.

Aldemir, M. (2018). *Elektronik Para ve Blockchain'in Finansal Yönetim Üzerine Etkileri.* Yayımlanmamış Yüksek Lisans Tezi, Maltepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications,* 9(7), 241-246.

Alnıaçık, B. (2019). Kripto Paraların Dünya ve Türkiye'deki Güncel Durumu Üzerine Bir İnceleme. *Research Studies Anatolia Journal,* 2(4), 21-30.

Ammous, S. (2019). *Bitcoin Standardı Merkez Bankacılığına Adem-i Merkeziyetçi Alternatif.* (Çev. Evgin Serbest). İstanbul: Liber Plus Yayınları. (Eserin orijinali 2018'de yayımlandı).

Andrianto, Y. and Diputra, Y. (2017). The Effect of Cryptocurrency on Investment Portfolio Effectiveness. *Journal of Finance and Accounting,* 5(6), 229-238.

Aslantaş Ateş, B. (2016). Kripto Para Birimleri, Bitcoin ve Muhasebesi. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 7(1), 349-366.

Aslanyürek, C. (2018). *Şifreleme Algoritmalarının Hızını Etkileyen Faktörler.* Yayımlanmamış Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Aşar, A. O. (2016). *Türkiye'de Takas Sistemi ve Uygulamadaki Problemlerle İlgili Bir Uygulama.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Atabaş, H. (2018). *Blokzinciri Teknolojisi ve Kripto Paraların Hayatımızdaki Yeni Yeri.* (1. Baskı). İstanbul: Ceres Yayınları.

Atay, G. (2013). *Dünyada ve Türkiye'de Altın Piyasaları ve Türkiye'de Altın Fiyatlarını Etkileyen Faktörlerin İncelenmesi.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Atik, M., Köse, Y., Yılmaz, B.ve Sağlam, F. (2015). Kripto Para: Bitcoin ve Döviz Kurları Üzerine Etkileri. *Bartın Üniversitesi İİBF Dergisi,* 6(11), 247-261.

Avunduk, H. ve Aşan, H. (2018). Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme. *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 33(1), 379-384.

Ayvaz Güven, E. T. ve Ayvaz, Y. Y. (2016). Türkiye'de Enflasyon ve İşsizlik Arasındaki İlişki: Zaman Serileri Analizi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Degisi,* 13(1), 241-262.

Azman, F. (2018). Kripto Para., Alptekin, V., Metin, İ. ve Akcan, A. T. (Editörler). *Kripto Para Ekonomisi.* Birinci Baskı. Konya. Eğitim Yayınevi, ss.59-74.

Bağdiken, M. ve Beşer, B. (2009). Ekonomik Büyüme ile Kamu Harcamaları Arasındaki Nedensellik İlişkisinin Wagner Tezi Kapsamında Bir Analizi: Türkiye Örneği. *Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Dergisi,* 5(9), 1-17.

Bakan, İ. ve Şekkeli, Z. H. (2019). Blok Zincir Teknolojisi ve Tedarik Zinciri Yönetimindeki Uygulamaları. *Uluslararası Toplum Araştırmaları Dergisi,* 11(8), 2847- 2877.

Baliga, A. (2017). Understanding Blockchain Consensus Models. *Persistent Systems White Paper,* 1-14.

Ballı, P. E. (2019). *Türkiye'de Doğrudan Yabancı Yatırımların Ekonomik Büyüme ve İstihdama Etkisi.* Yayımlanmamış Yüksek Lisans Tezi, Bandırma Onyedi Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Bandırma.

Baran, P. (1964). On Distributes Communications Networks. *IEEE Transactions on Communications Systems,* 12(1), 1-9.

Barışık, S. ve Kesikoğlu, F. (2006). Türkiye'de Bütçe Açıklarının Temel Makroekonomik Değişkenler Üzerine Etkisi (1087-2003 VAR, Etki-Tepki Analizi, Varyans Ayrıştırması). *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* 61(4), 59-82.

Bartos, J. (2015). Does Bitcoin Follow the Hypothesis of Efficient Market?. *International Journal of Sciences,* 4(2), 10-23.

Başkök, M. D. (2007). *AES Şifreleme Algoritmasının Modellenmesi.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Beck, R. (2018). Beyond Bitcoim: The Rise of Blockchain World. *IEEE Computer,* 51(2), 54-58.

Berg, A. and Berg, C. (2017). Exit, Voice, and Forking. SSRN 3081291.

Bhanot, R. and Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and ItsApplications,* 9(4), 289-306.

Bhosale, J. and Mavale, S. (2018). Volatility of Select Crypto-currencies: A Comparison of Bitcoin, Ethereum and Litecoin. *Pune Annual Research Journal of Symbiosis Centre for Management Studies,* 6, 132-141.

Bondarenko, O., Kichuk, O. and Antonov, A. (2019). The Possibilities of Using Investment Tools Based on Cryptocurrency in the Development of the National Economy, *Baltic Journal of Economic Studies,* 5(2), 10-17.

Boran Güneysu, N. ve Memiş, B. (2018). Bitcoin ve İcra Hukuku. *Fides Law Review,* 1, 82-92.

Bouoiyour, J. and Selmi, R. (2016). Bitcoin: A Beginning of A New Phase?. *Economics Bulletin,* 36(3), 1430-1440.

Bozkurt, Ö. Ö. (2005). *Eliptik Eğri Şifreleme Kullanarak Güvenli Soket Katmanı Protokolü'nün Gerçeklenmesi ve Performansının Değerlendirilmesi.* Yayımlanmamış Doktora Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Brill, A. and Keene, L. (2014). Cryptocurrencies: The Next Generation of Terrorist Financing? *Defence Against Terrorism Review,* 6(1), 7-30.

Bunjaku, F., Gjorgieva-Trajkovska, O. and Miteva-Kacarski, E. (2017). Cryptocurrencies-Advantages and Disadvantages. *Journal of Economics,* 2(1), 31-39.

Buterin, V. (2014). A Next Generation Smart Contract & Decentralized Application Platform. Ethereum *White Paper,* 1-36.

Büyükakın, F., Bozkurt, H. ve Cengiz, V. (2009). Türkiye'de Parasal Aktarımın Faiz Kanalının Granger Nedensellik ve Toda-Yamamota Yöntemleri ile Analizi. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 33, 101-118.

Büyükkaya, E. (2017). *Raspberry Pi Üzerinde AES Algortimasına Yan Kanal ve Ölçüm İyileşmesi.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Catalini, C. and Gans, J. S. (2018). *Some Simple Economics of the Blockchain,* NBER Working Paper No: 22952, National Bureau of Economic Research Working Paper Series, Cambridge.

Ceylan, M. E. (2019). *Bitcoin Ekonomisi: Kripto Para Bitcoin'in Finans Sektörü İçindeki Yeri.* Yayımlanmamış Yüksek Lisans Tezi, Batman Üniversitesi Sosyal Bilimler Enstitüsü, Batman.

Chohan, U. W. (2017). *A History of Bitcoin.* Discussion Paper Series: Notes on the 21st Century.

Chu, J., Chan, S., Nadarajah, S. and Osterrieder, J. (2017). GARCH Modelling of cryptocurrencies. *Journal of Risk and Financial Management,* 10(17), 2-15.

Chuen, D. L. K., Guo, L. and Wang, Y. (2018). Cryptocurrency: A New Investment Opportunity?. *Publishes in Journal of Alternative Investments,* 20(3), 16-40.

Crosby. M., Nachiappan, Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). *BlockChain Technology: Beyond Bitcoin.* Applied Innovation Review, 2, 6-19.

Çağlarırmak Uslu, N. (2013). Para ve Finansal Sistem., Çağlarırmak Uslu, N. ve Özdemir, B. K. (Editörler). *Para ve Banka.* Üçüncü Baskı. Eskişehir: Anadolu Üniversitesi Yayınları, ss.2-29.

Çarkacıoğlu, A. (2016). *Kripto-Para Bitcoin.* Araştırma Raporu, Sermaye Piyasası Kurulu Araştırma Dairesi.

Çeker, S. M. (2018). *Kripto Paralar ve Ekonomik Etkileri.* Yayımlanmamış Bitirme Tezi, Yıldız Teknik Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, İstanbul.

Çelik, T. T. ve Taş, O. (2007). Etkin Piyasa Hipotezi ve Gelişmekte Olan Hisse Senedi Piyasaları, *İTÜ Dergisi,* 4(2), 11-22.

Çetin, M. ve Şeker, F. (2014). Ekonomik Büyüme ve Dış Ticaretin Çevre Kirliliği Üzerindeki Etkisi: Türkiye için Bir ARDL Sınır Testi Yaklaşımı. *Yönetim ve Ekonomi,* 21(2), 213-230.

Çetiner, M. (2018). Bitcoin (Kripto Para) ve Blok Zincirin Yeni Dünyaya Getirdikleri. *İstanbul Journal of Social Sciences,* 20, 1-16.

Çetinkaya, Ş. (2018). Kripto Paraların Gelişimi ve Para Piyasasındaki Yerinin Swot Analizi ile İncelenmesi. *Uluslararası Ekonomi ve Siyaset Bilimleri Akademik Araştırmalar Dergisi,* 2(5), 11-21.

Çiydem, F. N. ve Selçuk, H. (2019, 27-28 Nisan). *Kripto Paralar ve Blockchain Teknolojisinin Kullanım Alanları, İslami Finansta Uygulanabilmesi.* Uluslararası İslam Ekonomisi, Finans ve Etik Kongresinde sunuldu, İstanbul.

Çütçü, İ. ve Kılıç, Y. (2018). Bitcoin Fiyatları İle Dolar Kuru Arasındaki İlişki: Yapısal Kırılmalı Zaman Serisi Analizi. *Yönetim ve Ekonomi Araştırmaları Dergisi,* 16(4), 349-366.

Demartino, I. (2018). *Bitcoin Rehberi Kripto Paralar Hakkında Bilmek İstediğininz Her şey* (Çev. Kübra Tekneci). İstanbul: Epsilon Yayınevi. (Eserin orijinali 2016'da yayımlandı).

De Roode, G., Ullah, I. And Havinga, P. J. M. (2018). How to Break IOTA Heart by Replaying?. *2018 IEEE Globecom Workshops (GC Wkshps),* 1-7.

Devries, P. D. (2016). An Analysis of Cryptocurrency, Bitcoin and The Future. *International Journal of Business Management and Commerce,* 1(2), 1-9.

Dirican, C. ve Canöz, İ. (2017). Bitcoin Fiyatları ile Dünyadaki Başlıca Borsa Endeksleri Arasındaki Eşbütünleşme İlişkisi: ARDL Modeli Yaklaşımı İle Analiz. *Journal of Economics, Finance and Accounting- (JEFA),* 4(4), 377-392.

Divya, M. and Biradar, N. B. (2015). IOTA-Next Generation Block chain. *International Journal of Engineering and Computer Science,* 7(4), 23823-23826.

Dizkırıcı, A. S. ve Gökgöz, A. (2018). Kripto Para Birimleri ve Türkiye'de Bitcoin Muhasebesi. *Journal of Accounting, Finance and Auditing Studies,* 4(2), 92-105.

Doğan, A. Y. (2008). *AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Drozd, O., Lazur, Y. and Serbin, R. (2017). Theoretıcal And Legal Perspectıve On Certaın Types Of Legal Lıabılıty In Cryptocurrency Relatıons. *Baltic Journal of Economic Studies,* 3(5), 221-228.

Dulupçu, M. A., Yiyit, M., Genç, A. G. (2017). Dijital Ekonominin Yükselen Yüzü: Bitcoin'in Değeri İle Bilinirliği Arasındaki İlişkinin Analizi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 22(15), 2241-2258.

Durairajan, M. S. and Saravanan, R. (2014). Biometrics Based Key Generation Using Diffie Hellman Key Exchange for Enhanced Security Mechanism. *International Journal of ChemTech Research,* 6(9), 4359-4365.

Durmuş, S. ve Polat, M. Ş. (2018). Sanal Para Bitcoin. *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 9(18), 659-673.

Dülgerler, M, and Sarısakal, M. N. (2003). A Secure E-Mail Application Using the ElGamal Algorithm: MD Message Controller. *Istanbul University Journal of Electrical & Electronics Engineering,* 3(1), 801-806.

Dwyer, G. P. (2014). The Economics of Bitcoin and Similar Private Digital Currencies. *Munich Personal RePEc Archive (MPRA),* Paper No: 57360.

Elbahrawy, A., Alessandretti, L., Kandler, A., Pastor- Satorras, R. and Baronchelli, A. (2017). Evolutionary Dynamics of The Cryptocurrency Market. *Royal Society Open Science,* 4(170623).

Eriş, M. ve Kaya, M. (2016). Cryptolocker Saldırılarının İncelenmesi. *İleri Teknoloji Bilimleri Dergisi,* 5(2), 112,119.

Erkuş, H. ve Gümüş, A. (2019). Blockchain ve Kripto Paraların Kullanımı Üzerine Bir Değerlendirme. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi,* 7(2), 41-49.

Erözel Durbilmez, S. ve Yılmaz Türkmen, S. (2019). Blockchain Teknolojisi ve Türkiye Finans Sektöründeki Durumu. *Finans Ekonomi ve Sosyal Araştırmalar Dergisi,* 4(1), 30-45.

Fabian, B., Ermakova, T. and Sander, U. (2016). *Anonymity in Bitcoin – The Users' Perspective.* Draft –Thirty Seventh International Conference on Information Systems, Dublin.

Fatima, A. and Tiwari, V. K. (2018). Bitcoin Cryptocurrency: A Review. *American Research Journal of Computer Science and Information Technology,*3(1), 1-8.

Gandal, N. and Halaburda, H. (2014). *Competition in the Cryptocurrency Market.* Bank of Canada Working Paper No: 2014-33, Bank of Canada, Ottowa.

Gao, J., Asamoah, K. O., Sifah, E. B., Smahi, A., Xia, Q. Xia, H., Zhang, X. and Dong, G. (2018). Gridmonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. *IEEE Access,* 6, 9917-9925.

Gençoğlu H. (2017). *Hibrit Şifreleme Algoritması.* Yayımlanmamış Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Gibbs, T. and Yordchim, S. (2014). Thai Perception on Litecoin Value. *World Academy of Science, Engineering and Technology International Journal of Economics and Management Engineering,* 8(8), 2634-2636.

Gipp, B., Meuschke, N. and Gernandt, A. (2015, March). *Decentralized Trusted Timestamping Using the Crypto Currency Bitcoin.* Proceedings of the iConference 2015, Newport Beach.

Goshwe, N. Y. (2013). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. *International Journal of Computer Science and Network Security,* 13(7). 9-13.

Gökçe, M. (2015). *Yapısal Kırılmalı Birim Kök Testleri ve İşsizlik Histerisi Üzerine Uygulama.* Yayımlanmamış Yüksek Lisans Tezi, İnönü Üniversitesi Sosyal Bilimler Enstitüsü, Malatya.

Güleç, Ö. F., Çevik, E. ve Bahadır, N. (2018). Bitcoin ile Finansal Göstergeler Arasındaki İlişkinin İncelenmesi. *Kırklareli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 7(2), 18-37.

Gültekin, Y. (2017). Turizm Endüstrisinde Alternatif Bir Ödeme Aracı Olarak Kripto Para Birimleri: Bitcoin. *Güncel Turizm Araştırmaları Dergisi,* 1(2), 96-113.

Gültekin, Y. ve Bulut, Y. (2016). Bitcoin Ekonomisi: Bitcoin Eko-Sisteminden Doğan Yeni Sektörler ve Analizi. *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 3(3), 82-92.

Günay, H. F. ve Kargı, V. (2018). Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirimesi. *Journal of Life Economics,* 5(3), 61-76.

Gündüz, A. ve Tepeci, M. (2018). Blokzinciri Teknolojisi., Alptekin, V., Metin, İ. ve Akcan, A. T. (Editörler). *Kripto Para Ekonomisi.* Birinci Baskı. Konya. Eğitim Yayınevi, ss.37-58.

Güven, V. ve Şahinöz, E. (2018). *Blokzincir- Kripto Paralar- Bitcoin Satoshi Dünyayı Değiştiriyor.* (2. Baskı). İstanbul: Kronik Kitap Yayıncılık.

Harn, L., Mehta, M. and Hsin, W. J. (2004). Integrating Diffie-Hellman Key Exchange into the Digital Signature Algorithm (DSA). *IEEE Communications Letters,* 8(3), 198-200.

Harwick, C. (2016). Cryptocurrency and the Problem of Intermediation. *The Independent Review,* 20(4), 569-588.

Hassanpour, A. A. (2015). *Asal Sayıların Şifreleme Teorisindeki Uygulamaları.* Yayımlanmamış Yüksek Lisans Tezi, Atatürk Üniversitesi Fen Bilimleri Enstitüsü, Erzurum.

Hayes, A. (2015). *Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin.* Ninth Mediterranean Conference on Information Systems (MCIS), Samos, Greece.

Hayes, A. S. (2017). Cryptocurrency Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin. *Telematics and İnformatics,* 34(7), 1308-1321.

Heid, A. (2013). Analysis of Cryptocurrency Markeyplace. *Retrieved February,* 15.

Hileman, G. and Rauchs, M. (2017). *Global Cryptocurrency Benchmarking Study,* Cabridge Centre for Alternative Finanse, University of Cambridge Judge Business School, 33.

Houber, R. and Snyers, A. (2018). *Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion.* Policy Department for Economic, Scientific and Quality of Life Policies, PE 619.024.

İda, A. (2017). *Bitcoin Hakkında Güncel Her şey.* (1. Baskı). İstanbul: Bizim Gezegen Yayınları.

İğde, E. (2010). *Yapısal Değişiklik Altında Birim Kök Testleri ve Bazı İktisadi Değişkenler Üzerine Uygulamalar.* Yayımlanmamış Yüksek Lisans Tezi, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Adana.

İnci S. ve Alper İ. (2018). *Bitcoin Devrimi Değişen Dünya Ekonomisinde Kripto Para Sistemi, Blockchain, Altcoinler.* (1. Basım). Ankara: Elma Yayınevi.

İşler, B. ve Takaoğlu, M. ve Küçükali, U. F. (2019). Blokzincir ve Kripto Paraların İnsanlığa Etkileri. *Yeni Medya Elektronik Dergi- eJNM,* 3(2), 71-83.

Kabir, M. A., Saidin, S. Z. and Ahmi, A. (2015). *Adoption of e-Payment Systems: A Review of Literature.* Proceedings of the International Conference on E-Commerce, Kuching, Malaysia, 112-120.

Kahraman, A. (2019). *Türk ve Avrupa Birliği Düzenlemeleri Işığında Elektronik Para.* Yayımlanmamış Yüksek Lisans Tezi, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Kalaitzis, A. (2018). *Bitcoin-Monero Analysis: Pearson and Spearman Correlation Coefficients of Cryptocurrencies.* Unpiblished Master's Thesis, Mälardalen University, Sweden.

Kamacı, A. ve Özden, N. M. (2019). Lale Çılgınlığı ve Kripto Para İlişkisi. *International Academic Journal,* 3(1), 26-40.

Kanat, E. ve Öget, E. (2018). Bitcoin İle Türkiye ve G7 Ülke Borsaları Arasındaki Uzun ve Kısa Dönemli İlişkilerin İncelenmesi. *Finans Ekonomi ve Sosyal Araştırmalar Dergisi,* 3(3), 601-614.

Kaplanhan, F. (2018). Kripto Paranın Türk Mevzuatı Açısından Değerlendirilmesi: Bitcoin Örneği. *Vergi Sorunları Dergisi,* 353, 105-123.

Karaçalı, C. (2019). *Kripto Paraların Muhasasebeleştirilmesi: Bir Uygulama.* Yayımlanmamış Yüksek Lisans Tezi, Bartın Üniversitesi Sosyal Bilimler Enstitüsü, Bartın.

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

Kardaş, S. ve Kiraz, M. S. (2018). Bitcoin'de Mahremiyeti Sağlama Yöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 4(1), 1-9.

Karzan, A. A. (2013). *Konu Tabanlı Etmen Göçü İçin Güvenlik Yapısı.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Bilişim Enstitüsü, İstanbul.

Katrancı, Y. ve Özdemir, A. Ş. (2013). RSA Şifrelemesi Yardımıyla Modüler Aritmetik Konusunun Pekiştirilmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi,* 3(1). 149-186.

Kesebir, M. ve Günceler, B. (2009). Kripto Para Birimlerinin Parlak Geleceği. *Iğdır Üniversitesi Sosyal Bilimler Dergisi,* 17, 601-621.

Kızıl, E. (2019). Türkiye'de Kripto Paranın Vergilendirilmesi ve Muhasebeleştirilmesi. *Mali Çözüm Dergisi,* 29(155), 179-196.

Kim, C., Tao,W., Shin, N. and Kim, K. S. (2010). An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems. *Electronic Commerce Research and Applications,* 9, 84-95.

Kirdaban, M. İ. (2005). *Ödemeler Sistemlerindeki Gelişmelere ve Ödeme Sistemlerinin Finansal Sistem İstikrarı Üzerindeki Etkileri.* Uzmanlık Yeterlilik Tezi, Türkiye Cumhuriyeti Merkez Bankası Bankacılık ve Finans Kuruluşlar Genel Müdürlüğü, Ankara.

Koçoğlu, Ş., Çevik, Y. E. ve Tanrıöven, C. (2016). Bitcoin Piyasalarının Etkinliği, Likiditesi ve Oynaklığı. *İşletme Araştırmaları Dergisi,* 8(2), 77-97.

Kodaz, H. ve Botsalı, F. M. (2010). Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması. *Selçuk-Teknik Dergisi,* 9(1), 10-23.

Konukseven, S. ve Özen, T. (2018). *50 Yıllık Hayal Bitcoin.*(1. Baskı). İstanbul: Mediacat Yayıncılık.

Kösesoy, İ. (2019). Nesnelerin İnterneti Güvenliğinde Blok Zinciri Uygulamaları. *Veri Bilimi Dergisi,* 2(1), 1-9.

Kula, G. Ç. (2009). *Gelişmiş Şifreleme Standardı Blok Şifreleme Algoritmasının Bir Mikroişlemci Üzerinde Gerçeklemesine Yan Kanal Saldırısı.* Yayımlamlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Kumar, Y., Munjal, R. and Sharma, H. (2011). Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. *International Journal of Computer Science and Management Studies,* 11(3), 60-63.

Kurt, L. (2018). *Kripto Para Bitcoin Finansal Özgürlüğün Eşiğinde.* (2. Baskı). Ankara: Karina Yayınevi.

Lee, D. K. C., Guo, L. and Wang, Y. (2018). Cryptocurrency: A New İnvestment Opportunity ?. *Journal of Alternative İnvestments,* 20(3), 16-40.

Luther, W. J. (2016). Bitcoin and The Future of Digital Payments. *The Independent Review,* 20(3), 397-404.

Luther, W. J. ve White, L. H. (2014). *Can Bitcoin Become a Major Currency?*. George Mason University Department of Economics Working Paper No: 14-17.

Mahajan, P. and Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology Network, Web & Security,* 13(15), 14-22.

Mendi, A. F. ve Çabuk, A. (2018). Bitcoin'in Arkasındaki Güç: Blockchain. *GSI Journal Serie C: Advancements in Information Sciences and Technologies,* 1(1), 19-23.

Metin, İ. ve Alptekin, V. (2018). Türkiye'de Önde Gelen Kripto Para Borsaları., Alptekin, V., Metin, İ. ve Akcan, A. T. (Editörler). *Kripto Para Ekonomisi.* Birinci Baskı. Konya. Eğitim Yayınevi, ss.177-190.

Milutinovic, M. (2018). Cryptocurrency. *Ekonomika,* 64(1), 105-122.

Minni, R., Sultania, K., Mishra, S. and Vincent, D. R. (2013, Temmuz). *An Algorithm to Enhance Security in RSA*. Paper presented at the Fourth International Conference on Computing, Communications and Networking, Tiruchengode, India.

Nair, M. and Cachanosky, N. (2016). Entrepreneurship and Bitcoin: Breaking the Network Effect. *2017. Review of Austrian Economics,* 30(3).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org.

Nebil, F. S. (2018). *Bitcoin ve Kripto Paralar Sistemi Yıkan Bir Araç Olabilecek mi? Dünyada ve Türkiye'deki Gelişmeler* (1. Baskı). İstanbul: Pusula Yayıncılık.

Özaydın, Ö. (2018). *Türkiye'de Enerji Tüketimi ve Seçilmiş Makroekonomik Değişkenler Arasındaki İlişkiler: ARDL Sınır Testi Analizi.* Yayımlanmamış Doktora Tezi, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

Özbaş, M. Y. (2019). Elektronik Para ve Sanal Para: Bitcoin Geleceğin Para Birimi Olabilir mi?. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi,* 1, 85-104.

Özcan, D. (2019). *Blokzincir Mimarisi ve Merkezi Olmayan Uygulamalar.* (1.Baskı). İstanbul: Pusula Yayıncılık.

Özden, F. (2019). *Fıkhî Açıdan Kripto Para Sistemi Bitcoin Örneği.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Öztemur, M. (2012). *AES Algoritmasının Bir Gerçeklemesine Güç Analizi Saldırıları.* Yayımlanmamış Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Öztürk, N. ve Koç, A. (2006). Elektronik Para, Diğer Para Türleriyle Karşılaştırılması ve Olası Etkileri. *Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Sosyal ve Ekonomik Araştırmalar Dergisi,* 11, 207-243.

Pamuk, M. ve Bektaş, H. (2014). Türkiye'de Eğitim Harcamaları ve Ekonomik Büyüme Arasındaki İlişki: ARDL Sınır Testi Yaklaşımı. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,* 2(2), 77-90.

Parasız, İ. (1998). *Modern Para Teorisi.* (1. Baskı). Bursa: Ezgi Kitabevi Yayınları.

Patil, A. and Goudar, R. (2013). A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices. *International Journal of Scientific & Rechnology Research,* 2(8), 61-65.

Paya, M. (2013). *Para Teorisi ve Para Politikası.* (6. Baskı). İstanbul: Türkmen Kitabevi.

Pichl, L. and Kaizoji, T. (2017). Volatility Analysis of Bitcoin Price Time Series. *Quantitative Finance and Economics,* 1(4), 474-485.

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros & M. Zhegu (Eds.) *Research Handbook on Digital Transformations.* Edward Elgar.

Rabah, K. (2016). Digital Cryptoeconomics Powered by Digital Cryotocurrency. *Mara Research Journal of Computer Science and Information Security,*1(1), 107-131.

Rihan, S. D., Khalid, A. and Osman S. E. F. (2015). A Performance Comparison of Encryption Algorithms AES amd DES. *International Journal of Engineering Research & Technology (IJERT),* 4(12), 151-154.

Rose, C. (2015). The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution. *International Business & Economics Research Journal,* 14(4), 617-622.

Prypto. (2018). *Bitcoin for Dummies.* (Çev. Erişah Arıcan, Başak Tanınmış Yücememiş, Gökhan Işıl ve Aclan Omağ). Ankara: Nobel Akademik Yayıncılık. (Eserin orijinali 2016'da yayımlandı).

Salviotti, G., De Rossi, L. M. and Abbatemarco, N. (2018). *A Structured Framework to Assess the Business Application Landscape of Blockchain Technologies.* Proceedings of the 51st Hawaii International Conference on System Sciences, 3467-3476.

Sankar, L. S., Sindhu, M. and Sethumadhavan, M. (2017). *Survey of Consenses Ptotocols on Blockchain Applications.* Paper presented at the 2017 International Conference on Advanced Computing and Communication Systems, Coimbatore, India.

Sarı, A. (2008). Parasalcı Görüşe Göre Türkiye'de Ödemeler Bilançosu Dengesinin Sağlanmasında Otomatik Denkleşme Mekanizmalarının Etkinliği. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi,* 9(2), 1-12.

Sarıkaya, K. S. (2005). *Elektronik İmza Güvenliği ve Güvenlik Standartları Çerçevesinde Düzenleyici Yaklaşımlar.* Telekomünikasyon Kurumu Uzmanlık Tezi, Ankara.

Sarısakal, M. N., Marangoz, K. G. ve Uçan, O. N. (2001). Elektronik Ticaret'te Sayısal İmzanın Kullanımı. *Istanbul University Engineering Faculty Journal of Electrical & Electronics,* 1(2), 169-178.

Sasi, S. B., Dixon, D. and Wilson, J. (2014). A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security. *IOSR Journal of Engineering (IOSRJEN),* 4(3),1-4.

Saygı, Z. Ve Yeşil. S. (2006, 7-8 Aralık). *Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar.* I. Ulusal Elektronik İmza Sempozyumunda sunuldu, Ankara.

Scherer, M. (2017). *Performance and Scalability of Blockchain Network and Smart Contracts.* Unpublished master's thesis, Umea University Department of Computing Science and Engineering, Sweden.

Scott, B. (2016). *How Can Cryptocurrency and Blockchain Technology Play A Role in Building Social and Solidarity Finance?*.UNRISD Working Paper NO: 2016-1, United Nations Research Institute for Social Development, Geneva.

Selçuk, M. (2019). Kripto Para Birimleri ve Özellikleri; Bitcoin Örneği., Kaya, S., Selçuk, M. ve Bektaş, İ. (Editörler). *Kripto Para Birimleri.* Birinci Baskı. İstanbul. Ensar. ss. 21-37.

Singh, G. and Supriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications.* 67(1), 33-38.

Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence From Bitcoin, Ethereum, Dash, Litcoin, and Momero. *Journal of Economics and Financial Analysis,* 2(2), 1-27.

Söderberg, G. (2018). Are Bitcoin and Other Crypto-assets Money ?. *Sveriges Riskbank,* 5, 1-14.

Söderberg, G. (2018). What İs Money and What Type of Money Would an E-Krona Be ?. *Sveriges Riskbank Economic Review,* 3, 17-28.

Süslü, B. ve Baydur, C. M. (2002). Para İkamesi ve Türkiye'deki Gelişimi. *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* 27, 93-106.

Şahin, F. (2015). Modern Blok Şifreleme Algoritmaları. *İstanbul Aydın Üniversitesi Dergisi,* 26, 23-40.

Şahin, M. (2019). Kripto Para Yeni Bir Vergi Sığınağı mı ?. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 34, 169-181.

Şıklar, İ. (2004). *Para Teorisi ve Politikası.* (1.Basım). Eskişehir: T. C. Anadolu Üniversitesi Yayınları

Şen, F. (2019). Dağıtık Kayıt Teknolojisi. *Gümrük Ticaret Dergisi,* 17, 85-94.

Taçali, E. D. (2008). *Hisse Senedi Getirilerini Etkileyen Makroekonomik Faktörlerin Arbitraj Fiyatlama Modeli ile Analizi: Türkiye Örneği.* Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Takım, A. (2010). Türkiye'de GSYİH ile İhracat Arasındaki İlişki: Granger Nedensellik Testi. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 14(2), 315-330.

Tanrıverdi, M., Uysal, M. ve Üstündağ, M. T. (2019). Blokzinciri Teknolojisi Nedir ? Ne Değildir ? : Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi,* 12(3), 203-217.

Tarı, R. (2015). *Ekonometri.* (11. Basım). Kocaeli: Umuttepe Yayınları.

Tarı, R. ve Bozkurt, H. (2006). Türkiye'de İstikrarsız Büyümenin VAR Modelleri ile Analizi (1991.1-2004.3). *Ekonometri ve İstatistik,* 4, 12-28.

Taş, O. ve Kiani, F. (2018). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine Bir İnceleme. *Bilişim Teknolojileri Dergisi,* 11(4), 369-382.

Thakur, J. and Kumar, N. (2011). DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering,* 1(2), 6-12.

Thakur, K. K. and Banik, G. G. (2018). Cryptocurrency: Its Risks and Gains and The Way Ahead. *IOSR Journal of Economics and Finance,* 9(2), 38- 42.

Tirthani, N. and Ganesan. R. (2014). Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptohraphy. *IACR Cryptologye Print archive,* 49.

Tiryaki, A. (2013). Para ve Enflasyon., Afşar, M., Kılıçaslan, Y., Taşdemir, M., Fisunoğlu, M., Tiryaki, A., Ateş, S., Açıkalın, S. ve İslatince, H. (Editörler). *İktisada Giriş-II.* Birinci Baskı. Ankara. Anadolu Üniversitesi Yayınları, ss.114-138.

Tripathi, R. and Agrawal, S. (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC).* 1(6). 68-76.

Uçan, O. (2019). *Döviz Kuru Belirleme Modelleri Ekonometrik Zaman Serisi Uygulamaları.* (1.Baskı). İstanbul: Hiper Yayın.

Uçar, B. (2014). *Türkiye Ekonomisi için Cari Açık ve İktisadi Büyüme İlişkisi.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Uzgören, E. (2015). *Mikro İktisat Teorisi.* (1. Baskı). Kütahya: Academia Yayınevi.

Uzgören, N. ve Uzgören, E. (2005). Zaman Serisinde Sahte Regresyon Sorunu ve Reel Kamu Harcamalarına Yönelik Ekonometrik Model Uygulaması. *Akademik Bakış,* 5, 1-14.

Ümit, A. Ö. (2007). *Türkiye'de Bütçe Açığı ile Cari İşlemler Arasındaki İlişkilerin Zaman Serisi Analizi,* Yayımlanmamış Doktora Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

Ünsal, E. ve Kocaoğlu, Ö. (2018). Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. *Avrupa Bilim ve Teknoloji Dergisi,* 13, 54-64.

Vejačka, M. (2014). Basic Aspects of Cryptocurrencies. *Journal of Economy, Business and Financing,* 2(2), 75-83.

Vyas, C. A. and Lunagaria, M. (2014). Security Concerns and İssues for Bitcoin. *International Journal of Computer Applications,* 10-12.

Yadav, S. K. (2010). *Some Problems in Symmetric and Asymmetric Cryptography.* Unpoblished doctoral thesis, , Dr. B. R. Ambedkar University Department of Mathematics, Agra.

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018). *Blockchain Technology Overview.* National Institute of Standards and Technology Internal Report 8202, Gaithersburg, MD, USA.

Yakut, E. (2018). Dünyada Önde Gelen Kripto Para Borsaları., Alptekin, V., Metin, İ. ve Akcan, A. T. (Editörler). *Kripto Para Ekonomisi.* Birinci Baskı. Konya. Eğitim Yayınevi, ss.159-176.

Yalçın, S. (2019). Kripto Değişim Araçlarının Muhasebeleştirilmesi. *Muhasebe ve Finansman Dergisi,* 81, 101-120.

Yavuz, İ. (2008). *Eliptik Eğri Kriptosisteminin RFGA Üzerinde Gerçeklenmesi.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Yavuz, M. S. (2019). Ekonomide Dijital Dönüşüm: Blockchain Teknolojisi ve Uygulama Alanları Üzerine Bir İnceleme. *Finans Ekonomi ve Sosyal Araştırmalar Dergisi,* 4(1), 15-29.

Yerlikaya, T., Buluş, E. ve Buluş, N. (2006, 9-11 Şubat). *Asimetrik şifreleme algoritmalarında anahtar değişim sistemleri.* Akademik Bilişim Konferansında sunuldu, Denizli.

Yerlikaya, T., Gençoğlu, H., Emir, M. K., Çankaya, M. ve Buluş, E. (2013). RSA Şifreleme Algoritması ve Aritmetik Modül Uygulaması. *İstanbul Aydın Üniversitesi Dergisi,* 3(9), 95-104.

Yermack, D. (2013). *Is Bitcoin a Real Currency? An Economic appraisal.* NBER Working Paper No: 19747, National Bureau of Economic Research Working Paper Series, Cambridge.

Yeşilyurt, H. (2019). *Makroekonomik Değişkenlerin Bireysel Emeklilik Sistemi Üzerine Etkileri: Türkiye Örneği,* Yayımlanmamış Yüksek Lisans Tezi, Niğde Ömer Halisdemir Üniversitesi Sosyal Bilimler Enstitüsü, Niğde.

Yıldırım, B. (2010). *Yapısal Kırılma Durumunda Birim Kök Testleri ve Gelir Yakınsaması Analizi: Avrupa Birliği'ne Üye ve Aday Ülkeler için.*

Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Yıldırım, F. (2015). Kripto Paralar, Blok Zinciri Teknolojisi ve Uluslararası İlişkilere Muhtemel Etkileri. *Medeniyet Araştırmaları Dergisi,* 2(4), 81-97.

Yıldırım, K. (2014). *Makro İktisada Giriş.* (10. Baskı). Ankara: Nisan Kitabevi.

Yıldırım, K., Karaman, D. ve Taşdemir, M. (2014). *Makro Ekonomi.* (12. Baskı). Ankara: Seçkin Yayıncılık.

Yıldırım, S. (2013). *Türkiye'de Para ve Sermaye Piyasalarının Ekonomik Büyüme Üzerindeki Etkisi: ARDL Sınır Testi Yaklaşımı.* Yayımlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.

Yıldız, R. (2018). *ARDL Sınır Testi Yaklaşımı ile Türkiye'deki Konut Talebinin Modellenmesi.* Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.

Yılmaz, M. (2017). *Simetrik Şifreleme Algoritmalarının Kullanımı için Akıllı Bir Seçim Sistemi Geliştirilmesi.* Yayımlanmamış Yüksek Lisans Tezi, Muğla Sıtkı Koçman Üniversitesi Fen Bilimleri Enstitüsü, Muğla.

Yılmaz, M. ve Ballı, S. (2016). Veri Şifreleme Algoritmalarının Kullanımı İçin Akıllı Bir Seçim Sistemi Geliştirilmesi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 2(2), 18-28.

Yılmaz, Y. (2007). Kriptoloji Uygulamalarında Hukuki Boyut. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* 13 (1-2).

Yumuşaker, M. C. (2019). Kripto Para ve Tipleri, Bitcoin Olgusu ve Muhasebesi. *Uluslararası Toplum Araştırmaları Dergisi,* 12(18), 1007-1029.

Zamyatin, A., Wolter, K., Werner, S., Mulligan, C. E. A., Harrison, P. G. and Knottenbelt, W. J. (2017, September). *Swimming with Fishes and Sharks: Beneath the Surface of Queue-based Ethereum Mining Pools.* Paper presented at the 2015 IEEE 25th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems.

Zanjani, M. F. (2014). *Group Key Exchange Protocol Based on Diffie Hellman Technique in Ad hoc Network.* Unpublished master's thesis, Eastern Mediterranean University Department of Computer Engineering, Gazimağusa, North Cyprus.

Zheng, Z., Xie, S., Dai, H., Chen, X. And Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *Int. J. Web and Grid Services,* 14(4), 352-375.

Zheng, Z., Xie, S., Dai, H., Chen, X. And Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consenses, and Future Trends.* Paper presented at the 2017 IEEE 6th International Congress on Big Data, Hawaii, USA.

https://coinmarketcap.com

https://finance.yahoo.com

https://tr.investing.com

https://www.coinkolik.com

https://www.koindeks.com

https://www.tcmb.gov.tr

EKLER

Çalışmanın ekler kısmında kripto para türleri hakkında daha net bir bilgiye sahip olabilmek amacıyla kripto para piyasalarında en çok işlem gören ilk 100 kripto para birimi gösterilmiştir. Çalışmada verilen sıra numaraları en çok işlem gören para birimlerinin sıralaması dikkat edilerek verilmiştir. Ancak gün içerisinde piyasada birçok şifreli para birimi kendine yer bulmayı başardığı için bu sıralamanın her an değişebileceğinin de belirtilmesi gerekmektedir. Bu bilgilere ise coinmarketcap.com adresinden ulaşılmıştır.

Sıra	Kripto Para	Sembol	Sıra	Kripto Para	Sembol
1	Bitcoin	BTC	51	Nano	NANO
2	Ethereum	ETH	52	THETA	THETA
3	XRP	XRP	53	KuCoin Shares	KCS
4	Bitcoin Cash	BCH	54	DigiByte	DGB
5	Tether	USDT	55	Waves	WAVES
6	Bitcoin SV	BSV	56	Lisk	LSK
7	Litecoin	LTC	57	Centrality	CENNZ
8	EOS	EOS	58	Bytom	BTM
9	Binance Coin	BNB	59	Seele	SEELE
10	Stellar	XLM	60	BitTorrent	BTT
11	Monero	XMR	61	MCO	MCO
12	Cardano	ADA	62	MonaCoin	MONA
13	TRON	TRX	63	ICON	ICX
14	Tezos	XTZ	64	Molecular Future	MOF
15	Ethereum Classic	ETC	65	Komodo	KMD
16	Chainlink	LINK	66	Nervos Network	CKB
17	Dash	DASH	67	IOST	IOST
18	UNUS SED LEO	LEO	68	DxChain Token	DX
19	Cosmos	ATOM	69	HyperCash	HC
20	Neo	NEO	70	Siacoin	SC

21	Huobi Token	HT	71	LUNA	LUNA
22	IOTA	MIOTA	72	Verge	XVG
23	HedgeTrade	HEDG	73	Steem	STEEM
24	Crypto.com Coin	CRO	74	ABBC Coin	ABBC
25	Maker	MKR	75	Enjin Coin	ENJ
26	USD Coin	USDC	76	Nexo	NEXO
27	Zcash	ZEC	77	V Systems	VSYS
28	Ontology	ONT	78	DigixDAO	DGD
29	NEM	XEM	79	Bytecoin	BCN
30	VeChain	VET	80	BitShares	BTS
31	Basic Attention Token	BAT	81	Zilliqa	ZIL
32	Dogecoin	DOGE	82	Zcoin	XZC
33	Paxos Standard	PAX	83	Aeternity	AE
34	FTX Token	FTT	84	RIF Token	RIF
35	Decred	DCR	85	Kyber Network	KNC
36	Qtum	QTUM	86	Ardor	ARDR
37	Bitcoin Gold	BTG	87	Crypterium	CRPT
38	Synthetix Network Token	SNX	88	Matic Network	MATIC
39	Augur	REP	89	BlockStamp	BST
40	TrueUSD	TUSD	90	Energi	NRG
41	Ravencoin	RVN	91	Electroneum	ETN
42	0x	ZRX	92	Quant	QNT
43	Algorand	ALGO	93	iExec RLC	RLC
44	OKB	OKB	94	Silverway	SLV
45	Holo	HOT	95	Decentraland	MANA
46	Bitcoin Diamond	BCD	96	Status	SNT
47	OmiseGO	OMG	97	STASIS EURO	EURS
48	ZB Token	ZB	98	Ren	REN
49	Swipe	SXP	99	Golem	GNT
50	Horizen	ZEN	100	Grin	GRIN

Tablo'da koyu renk ile gösterilen kripto paralar madenciliğin yapıldığı diğerleri ise madenciliğin yapılmadığı kripto para birimleridir.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı ve Soyadı : Ecem TURGUT

Doğum Yeri : Niğde/ Merkez

Doğum Tarihi : 14.12.1995

E- mail : ecemtrgtt@gmail.com

EĞİTİM DURUMU

Yüksek Lisans :	Niğde Ömer Halisdemir Üniversitesi Sosyal Bilimler Enstitüsü İktisat Anabilim Dalı	2018-2020
Lisans :	Niğde Ömer Halisdemir Üniversitesi İktisat Bölümü	2015-2018
:	Necmettin Erbakan Üniversitesi İktisat Bölümü	2014-2015
Lise :	Remide Yılmaz Atabek Anadolu Lisesi	2009-2013

YABANCI DİL

İngilizce