T.C.

TİCARET BAKANLIĞI

BLOKZİNCİR TEKNOLOJİSİ VE GÜMRÜK İŞLEMLERİNDE BLOKZİNCİR UYGULAMA ALANLARININ İNCELENMESİ

Ticaret Uzmanlığı Tezi

Hazırlayan

Kadir GÜÇLÜ

Ankara

Eylül 2019

T.C.

TİCARET BAKANLIĞI

BLOKZİNCİR TEKNOLOJİSİ VE GÜMRÜK İŞLEMLERİNDE BLOKZİNCİR UYGULAMA ALANLARININ İNCELENMESİ

Ticaret Uzmanlığı Tezi

Hazırlayan

Kadir GÜÇLÜ

Danışman

Emrah YETİK

Ticaret Uzmanı

Ankara

Eylül 2019

ÖZET

Temeli yüzyıllar öncesinde atılan ve hizmetlerini geliştirerek insanların güvenini kazanmayı başaran finans ve bankacılık sektörüne bakış, 2008 yılında başlayan küresel finans krizi sebebiyle değişmiştir. Hem finans sektörü hem de düzenleyici ve denetleyici kurumlar güven kaybetmiştir. Aynı yıl Satoshi Nakamoto tarafından "Bitcoin: A Peer-to-Peer Electronic Cash System" başlıklı makale yayınlandı. Makalede Bitcoin; şifreleme temelli, tarafların doğrudan iletişimde olduğu, manipülasyonlara karşı gerekli önlemleri barındıran, aracı kurumların olmadığı ve merkezi sisteme bağlı olmadan çalışabilen para birimi olarak tanımlanmıştır. Her ne kadar Blokzincir kelimesine makalede yer verilmese de makale sayesinde Blokzincir kavramı doğmuştur. Bu tez, Blokzincir teknolojisinin gümrük işlemlerindeki uygulama alanlarına ilişkin genel bir bakış sunmaktadır.

Bu tezde ilk olarak Blokzincir teknolojisinin teknik altyapısı ve temel çalışma prensibi incelenmiştir. Daha sonra Blokzincir platformları ve küresel ölçekte Blokzincir uygulamaları araştırılmıştır. Sonuç olarak, teknolojinin gümrük işlemlerinde uygulanabileceği alanlar incelenecektir.

ABSTRACT

The view of the finance and banking sector, whose foundation was laid centuries ago and which gained the trust of people by improving its services, has changed due to the global financial crisis that started in 2008. Both the financial sector and regulatory and supervisory agencies have lost confidence. In the same year, Satoshi Nakamoto published an article titled “Bitcoin: A Peer-to-Peer Electronic Cash System”. In the article Bitcoin; It is defined as a currency based on cryptography, where the parties are in direct communication, which contains necessary measures against manipulations, that there are no intermediary institutions and can operate without being connected to the central system. Although the word Blokchains is not included in the article, the concept of Blokchains was born thanks to the article.This thesis provides an overview of the application areas of Blockchain technology in customs clearance.

In this thesis, firstly the technical infrastructure and basic working principle of the Blockchain technology is examined. Then, Blockchain platforms and Blockchain applications on global scale were investigated. As a result, the areas where the technology can be applied in customs procedures will be examined.

İÇİNDEKİLER

KISALTMALAR

API	: Uygulama Programlama Ara yüzü
BTC	: Bitcoin
DDK	: Dağıtık Defter-i Kebir
DG TAXUD	: AB Vergilendirme ve Gümrük Birliği Genel Müdürlüğü
EBP	: Elektronik Gümrük İşlemleri Dairesi Blokzincir Platformu
ETH	: Ethereum platformunun kripto para birimi Ether
EVM	: Ethereum Virtual Machine
GTCN	: Global Trade Connectivity Network
HKMA	: Hong Kong Para Otoritesi
ICC	: Uluslararası Ticaret Odası
IMF	: Uluslararası Para Fonu
ITAS	: Malta Yenilikçi Teknoloji Anlaşmaları ve Hizmetleri Kurumu
MAS	: Singapur Para Otoritesi
MDIA	: Malta Dijital Yenilik Kurumu
NIST	: Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü
NTP	: Networked Trade Platform
PoS	: Proof of Stake Protokolü
POS	: Elektronik alışveriş cihazı
PoW	: Proof of Work Protokolü
PTTEP	: Tayland petrol şirketi
SCB	: Tayland Siam Commercial Bank
SDK	: Yazılım Geliştirme Kiti
SDR	: Uluslararası Para Fonu tarafından oluşturulmuş özel çekme hakkı
SHA	: Güvenli Hash Algoritması

TPS : Tek Pencere Sistemi

WB : Dünya Bankası

WCF : Dünya Odaları Federasyonu

VFA : Malta Dijital Finansal Varlıklar Kurumu

ŞEKİL LİSTESİ

1. GİRİŞ

İnsan doğumdan ölüme kadar birçok bilgiyi hafızasında biriktirir. Ancak, gerek bilginin çoğalması gerekse çevresel ve biyolojik faktörler sebebiyle bütün bilgileri hafızasında tutması mümkün değildir. Unutkanlık sebebiyle maddi ya da manevi kayıplar yaşayan insanoğlu hafızasında sakladığı bilgiyi veriye dönüştürmüştür. Veri, işlenmemiş ham bilgilere verilen isimdir. Veriler tarih boyunca taş, kemik, deri ve kâğıt üzerine yazılarak günümüze kadar ulaşmıştır. Çinliler veriyi kâğıdın üzerine aktarabilmek için ahşap blokların üzerine harfleri oymuşlar ve bu bloklarla birlikte baskı yapmışlardır.15.yüzyıldan itibaren dökme demir harflerle dizgi ve matbaa gelişmiştir.

Yakın geçmişte elektriğin kullanılması, verinin bitlerle kaydedilmesi ve veri merkezlerinin kurulması ile birlikte disketler, hard diskler ve cd ler kullanılmış, akabinde hiçbir mekanik parçası olmayan diskler ortaya çıkmıştır. Nihayetinde, yer ve zaman fark etmeksizin veriyi bize ulaştıran bulut teknolojisi hayatımıza girmiştir. Bulut bir veri saklama ve aktarma aracı olup bu verinin hızlı bir şekilde aktarılması için ise fiber optik ağ alt yapıları kurulmuştur. Bütün bu gelişmeler olurken verinin herkes tarafından görülmesini engelleme ihtiyacı doğmuş, bu ihtiyacı karşılamak için ise kriptoloji bilimi kullanılmıştır. Kriptoloji, gizlilik bilimi olup tarih boyunca birçok medeniyet tarafından kullanılmıştır. Günümüzde ise kriptoloji, her alanda kullanılan bir bilim haline gelmiştir. Bilgisayarımızın açılışında, sim kartı cep telefonumuza taktığımızda, işyerimize girerken kimlik kartımızı okutmamızda, arabamızın kapısının kilidini açmamızda kriptoloji vardır.

Bilim insanları, küçük toplumlarda veri kaydına gerek olmadığını, herkesin yaptığı işin belli olduğunu, toplum fertlerine ait verilerin herkes tarafından bilindiğini ve toplumda bir düzen olduğunu belirtmektedir. Ancak topluluklar büyümeye başlayıp medeniyet meydana gelince küçük topluluklarda var olan düzeni sağlayabilmek neredeyse imkânsız hale gelmiştir. Oluşan medeniyetin düzen getirebilmesi adına veriler kanunlar, yönetmelikler ve sözleşmelerle kayıt altına alınmıştır. Bugün, toplumların sulh içerisinde yaşayabilmesi için kanun koyucu görevi üstlenen devletler, çıkardıkları kanunlar sayesinde toplum hayatının düzenli akışını sağlamış ve topluma

güven tesis etmiştir. Toplum fertleri, devletin oluşturduğu güven duygusu dışında sektörler açısından da güvene ihtiyaç duymaktadır. İşte bu noktada, güven tesis eden önemli sektörlerden biri bankacılık sektörüdür.

Yaklaşık 600 yıldır müşterilerine güven veren bankacılık sektörü, 2008 yılında meydana gelen büyük depremle yüzleşmiş ve Lehman Brothers ABD' de iflas etmiştir. İflas sonrası yaşanan küresel finans krizi sebebiyle dünya finans sisteminde pek çok değişim olmuş, ülke borsaları çökmüş, kredi derecelendirme kuruluşları itibar kaybetmiş, tüm dünyada yüzlerce banka batmış, binlerce şirket iflas etmiş ve milyonlarca kişi işsiz kalmıştır. Ancak her şeyden önemlisi insanların bankacılık ve finans sektörüne bakışları değişmiş ve bankalara duydukları güven ciddi şekilde zedelenmiştir.

Lehman Brothers' ın iflasından yaklaşık 2 ay sonra ABD' de Satoshi Nakamoto adındaki bir kişi tarafından "Bitcoin: A Peer-to-Peer Electronic Cash System" adıyla bir makale yayınlanmıştır. Makalede Bitcoin; hiçbir merkezi sisteme bağlı olmadan çalışabilen, şifreleme üzerine kurulu, iki tarafın birbiriyle doğrudan bağlantı kurduğu, kullanıcılarının ve dışarıdan kişilerin manipülasyona yönelik müdahalelerine karşı gerekli önlemlerin alındığı, aracı yapıların olmadığı dijital bir para birimi olarak anlatılmaktadır. Bu sistem, altında yatan güçlü şifreleme (kriptografi) teknikleri yardımıyla mutabakat üzerine kurulu şekilde veriyi kayıt altına almakta, kaydedilen veriyi tek bir merkez yerine tüm kullanıcılara birer kopyasını dağıtarak saklamaktadır. Nakamoto' nun makalesinde Blokzincir kelimesi hiç geçmese de, uygulanan yöntemler ve makalede yer verilen çeşitli şemalar sebebiyle Blokzincir kavramı doğmuş ve hızla gelişerek küresel ölçüde kabul gören temel bir teknolojik kavram haline gelmiştir. [1]

Makale aynı zamanda küresel kriz sonrası güven probleminin teknoloji sayesinde nasıl çözüleceği konusuna yeni bir boyut kazandırmaya çalışmaktadır. Bu çerçevede makalede kripto paraların en büyük özelliği olarak; arkasında para basma gücüne sahip otoritelere duyulan güven yerine matematik kurallarıyla temellendirilen ve bilgisayar algoritmalarına dayanan güven öne sürülmüştür. Satoshi Nakamoto' nun makalesine tezimizin sonraki bölümlerinde yer verilecektir.

2. TEMEL KAVRAMLAR

Blokzincir Teknolojisi hakkında detaylı bilgiler vermeden önce Veri, Veri Tabanı, Kriptografi, Bulut Bilişim, Node(Düğüm), Blok, Hashing(Özetleme), Merkle Ağaçları, Mutabakat Yapısı ve Dijital İmza kavramlarını açıklayalım.

2.1.Veri

Herhangi bir işleme tabi tutulmadan, gözlem veya ölçüm yöntemleri ile ortamdan elde edilen her türlü değerdir. [2]

Tek başına anlam ifade etmeyen, enformasyona ve bilgiye temel oluşturan ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgidir.

Tek başına işe yaramayan veri, toplanan diğer verilerle bir araya getirilip işlenince anlam kazanır. Veri; insanlar, hayvanlar, bitkiler ve doğa olayları gibi birçok tarafça üretilir. İnsan araştırma, anket, gözlem vb. yöntemlerle veri oluştururken mevsimlerin değişmesi, yağmur, yanardağ patlaması, deprem, hayvanların yaşamı gibi milyonlarca kayıt altına alınabilen ya da alınamayan veri üretilmektedir.

Verinin elde edilmesi kadar güvenli bir şekilde saklanması ve sonraki nesillere iletilmesi önem arz etmektedir. Bu sebeple tarih boyunca sayısız veri saklama ve iletme yöntemi kullanılmıştır. Bu yöntemlere ilişkin olarak günümüze ulaşan ilk bilgiler milattan önceki yıllara dayanır. M.Ö. 485–525 yıllarında yaşayan Yunan tarihçisi Herodot, bir çalışmasında Pers İmparatorluğu ile bir Yunan şehir devleti arasında geçen savaş sırasında gerçekleşen gizli bir iletişim metodunu anlatmıştır. Pers kralına ulaştırılacak gizli plan, taşıyacak kişinin kafası tıraş edilerek dövme ile yazılmış ve taşıyıcının saçları tekrar uzayıncaya kadar beklenmiştir. Böylece mesaj doğal yoldan gizlenmiştir. Görünürde yanında hiçbir şey bulunmayan taşıyıcı, özgürce seyahat edebilmiş ve ulaşması gereken yere vardığında kafasını tıraş edip taşıdığı mesajı göstermiştir. [3]

Taş ve kemik üzerine kazınan bilgiler, kâğıdın bulunması sonrasında matbaa ile hızlı şekilde çoğaltılan bilgiler, disket, cd, DVD, USB, optik diskler, harici diskler ve son olarak bulut teknolojisi ile bilginin korunması ve iletilmesi sağlanmıştır.

Bilgi kişiden kişiye saklanarak iletilebildiği gibi paylaşan taraflar dışındakilerin anlayamayacağı şekle de dönüştürülebilir. Bunun için steganografi, kriptoloji, sayısal damgalama, parmak izi ekleme gibi yöntemler kullanılabilir.

2.2.Veri Tabanı

Belirli bir konuda dizgeli biçimde düzenlenmiş ve bilgisayar ortamında korunan verileri ifade etmektedir. [4]

Yüzyıllar boyunca nesilden nesle bilgi aktarımının çeşitli yollarla yapıldığından bahsedilmişti. Asırlar öncesinde, yaşadıklarını kendinden sonraki nesillere sözlü olarak anlatan kişiler ve onların anlattığı kişiler veri tabanı görevi yaparken, yazının bulunması sonrası taş ve kemik gibi maddeler, kâğıt ve matbaanın bulunmasından sonra ise kütüphaneler birer veri tabanı görevi üstlenmiştir. Günümüzde ise bilgisayar sistemleri kütüphane görevi üstlenmekte olup veri tabanı işlevi görmektedir.

Kamu kurumları ve özel sektörün çağa uyum sağlaması ve geleceğe dönük politikalarını belirlemesi için veri tabanında güvenli şekilde muhafaza edeceği verilere ve o verilerle yapacağı analizlere ihtiyaç vardır. Nitekim Bakanlığımız veri tabanında yer alan veriler kullanılarak yapılan analizler sonrasında dış ticaret süreçlerinde iyileştirmeler ve özellikle kaçakçılıkla mücadelede ilerleme kaydedilmektedir.

2.3.Kriptoloji

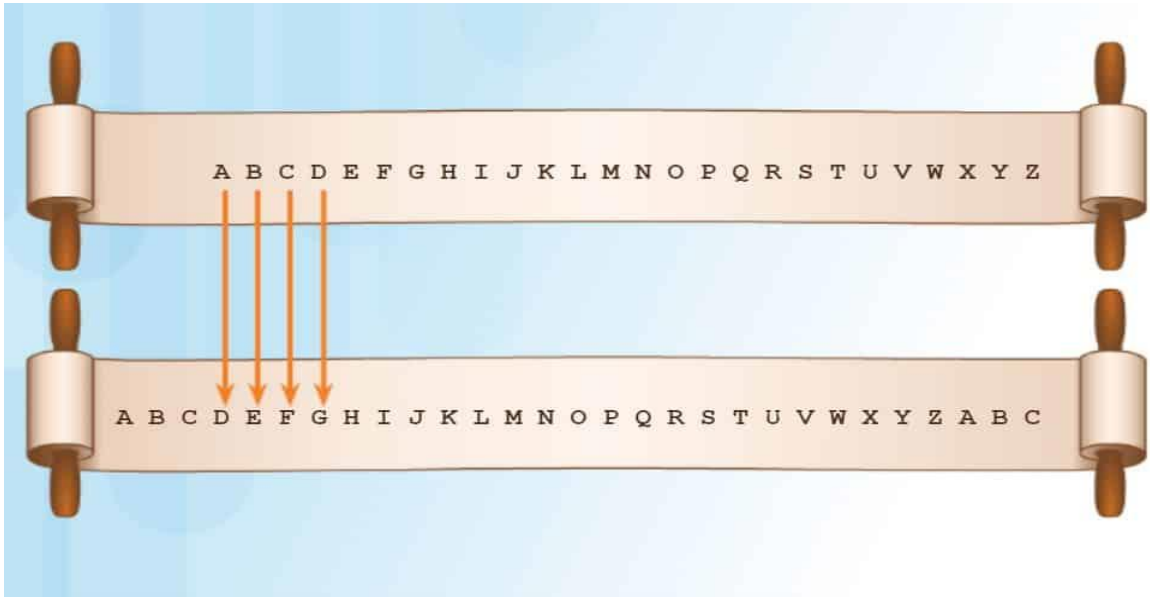
Kriptoloji kısaca şifre bilimi olup kriptografi, gizli kodları oluşturma ve bu kodları kırma bilimidir. Gizli belgeleri korumak için şifreleme tekniği asırlardır kullanılmaktadır. Firavunların mezarlarındaki yazıtlarda kullanılan semboller bilinen ilk kriptografik dönüşümler olup M.Ö. 475 yılında bilinen ilk kriptografik iletişim aracı olan “skytale”, Sparta’ da kullanılmıştır.

Şekil 1: Bilinen ilk kriptografik iletişim aracı Scytale

Kaynak: http://www.oxfordmathcenter.com (Erişim tarihi 20.07.2019)

Şifreleme ile herhangi bir veri bütünü, rastgele bir veri bütünü haline gelir ve gerçek veri sadece şifreleme yapılırken kullanılan anahtara sahip kişilerce görülebilir.

Julius Caesar' ın M.Ö. 60' lı yıllarda, iki takım alfabeyi alt alta koyarak kullanılan harfleri belirli bir sayıda kaydırarak mesajları güvence altına aldığı anlatılmaktadır. Burada kaydırılan yer sayısı anahtardır.



Şekil 2: Sezar Şifresi

Kaynak: https://www.indigodergisi.com (Erişim tarihi 20.07.2019)

2.4.Bulut Bilişim

Uzakta konumlandırılmış bilgisayarlara internet üzerinden erişilerek verilerin saklanması, işlenmesi ve kullanılması bulut bilişim olarak tanımlanabilir. Bulut bilişim sayesinde, kullanıcılar daha düşük bilgi teknolojileri maliyetleri ile veriler üzerinde işlem yapabilmektedir.

Herkesin her yerden istediği bilgiye erişebilmesi internet ile sağlanabiliyorken, yüksek bilgi işlem gücüne bulut bilişim ile ulaşılabilmektedir. [5]

Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)' e göre, "Bulut bilişim, yapılandırılabilir bilişim kaynaklarından oluşan ortak bir havuza uygun koşullarda ve isteğe bağlı olarak her zaman ve her yerden erişime imkân veren bir modeldir. Söz konusu kaynaklar (bilgisayar ağları, sunucular, veri tabanları, uygulamalar, hizmetler vb.) asgari düzeyde yönetimsel çaba ve hizmet alıcı-hizmet sağlayıcı etkileşimi gerektirecek kolaylıkta tedarik edilebilmekte ve elden çıkarılabilmektedir. [5]

Veri depolama, bilgisayar kullanan her kişinin temel ihtiyacıdır. Ancak verilerin bilgisayar ve telefon gibi aygıtlarda tutulması bu cihazların yavaşlamasına, boş alanlarının tükenmesine ve cihazların bozulması durumunda verilerin kaybolmasına sebep olmaktadır.

Bulut bilişim, verileri çevrimiçi bir platformda depolamaktadır. Başlıca bulut servisleri olan Dropbox, Yandex Disk, Google Drive veya Mega gibi bulut hizmetlerinden birine üye olunarak, kişiye verilen alan kadar veri yüklenebilmektedir. Bu veriler herhangi bir şekilde kaybolmayıp, üye olan kişi istemediği sürece üçüncü bir tarafça görüntülenemez ve veriler güvenli bir şekilde tutulup veri kaybı önlenmiş olur. Android, iOS ve Windows Phone gibi işletim sistemlerine sahip mobil aygıtların neredeyse tamamında bulut sistemi mevcuttur.

Bulut sistemleri, web protokollerini kullanarak kullanıcı-sunucu merkezli bir işlem gerçekleştirir. Bulut hesaplarına tüm bilgisayarlardan ve diğer akıllı aygıtlardan erişim sağlanabilir. Veriler firmaların sunucularında depolanır, kullanıcılar ise şifre yoluyla kendilerine ait olan alana ulaşarak dosya yükleyebilir, yeni veri girişi yapabilir

ya da var olan dosyaları değiştirebilir. Bulut hizmetine sahip kişi, uygun görmesi halinde şahsına ait dosyaları diğer kullanıcılarla paylaşabilir.

2.5.Node (Düğüm)

Node (düğüm) , Blokzincir ağındaki cihazlara verilen isimdir. İnternete bağlı olan ve IP adresi olduğu sürece bir bilgisayar, telefon ya da herhangi bir aktif cihaz node olabilir. Blokzincir teknolojisinin temeli düğümün çalışmasına bağlıdır. Bir düğümün görevi, bir blok kopyasını muhafaza ederek ve bazı durumlarda işlemleri işleyerek ağı desteklemektir. Her düğüm eşit olarak kabul edilir ancak belirli düğümlerin ağları desteklemekte farklı rolleri vardır. Tüm düğümler bağlı oldukları Blokzincir yapısının tüm kopyasını depolayamazlar veya tüm işlemleri doğrulayamazlar. Bu durumda parçalar halinde kopyalanır ve doğrulanır. Tam düğüm olarak adlandırılan makineler Blokzincir yapısının tam bir kopyasını indirebilir. Tüm düğümler birbirleri ile uyumlu olabilmek içi aynı fikir birliği protokolünü kullanmaktadır. [6]

2.6.Blok

Blokzincir yaklaşımında verilerin saklandığı yapılar blok olarak adlandırılır. Bu blok yapıları bir zincir şeklinde (zaman acısından doğrusal bir dizi yapısında) düzenlenir. Bu zincir kapsamındaki ilk blok yapısına “genesis (başlangıç)” blok denir. [1]

2.7.Hashing (Özetleme)

Blokzincir teknolojisinin güvenirliği, mükerrer işlemlerin veya kayıt altına alınan hileli verinin işlem şansı olmamasından kaynaklanmaktadır. Bu güvenirliğin en önemli parçası ise Hashing işlemidir. Hashing; herhangi bir girdiyi, matematik algoritma ile şifreli bir çıktı haline dönüştürme işlemidir.

Hashing sayesinde verilerin güvenliği önemli derecede artırılır. Kriptografik bir hash fonksiyonunun sahip olması gereken özellikler:

1- Aynı girdi her zaman aynı hash değerini üretir.

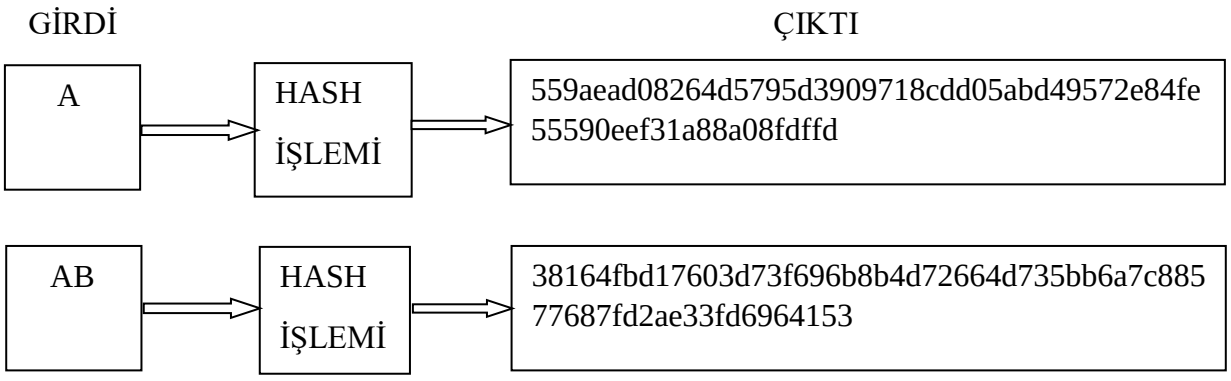
2- Farklı girdi aynı hash değerini vermeyecektir.

3- Hash değerinden girdiye erişmek olanaksızdır.

4- Girdide meydana gelen herhangi bir değişiklik, hash değerini tamamen değiştirecektir.

Kriptografik hash fonksiyonu, dijital imza şemaları, kimlik doğrulama kodları, parola işlem özet fonksiyonları ve içerik adresli depolama da dâhil olmak üzere pek çok uygulamada kullanılan temel bir kriptografi yöntemidir. [7]

Güvenli Hash Algoritması (SHA), bir dizi kriptografik hash işlevinden oluşur. SHA' nın daha iyi anlaşılabilmesi için kriptografik hash algoritma setinden birisi olan SHA-256 hesaplaması gerçekleştirelim.



Şekil 3: SHA-256 Hesaplaması

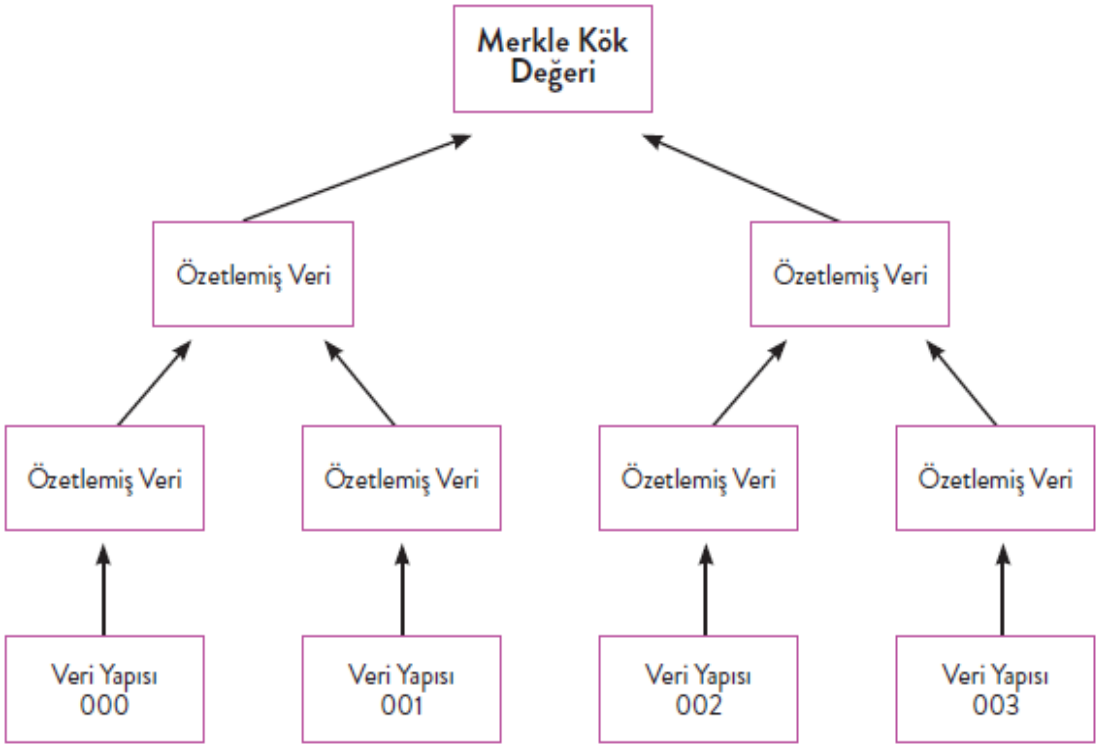
Kaynak: www.xorbin.com (Erişim tarihi 20.07.2019)

Güvenli Hash Algoritması(SHA) hesaplamamızda da görüldüğü üzere girdide meydana gelen en küçük değişiklik çıktının tamamen değişmesine sebep olmaktadır. Blokzincir teknolojisinin güvenirliğinin en önemli parçası budur.

Bitcoin, işlemlerinde SHA-256 isimli hash fonksiyonunu kullanmaktadır. SHA-256, girdinin uzunluğundan bağımsız olarak 256 bitlik (32 byte) bir çıktı üretir. Üretilen çıktıdan hareket ederek girdiye ulaşılamaz.

2.8.Merkle Ağaçları

Merkle ağacı, büyük veri kümelerini güvenli ve hızlı bir şekilde doğrulamak için kullanılan, güvenli Hashing (özetleme) yapısı üzerinde geliştirilmiş bir yaklaşımdır. Merkle ağaç yapısında ikili (binary) bir ağaç yapısı oluşturulup, en alt seviyeye veri kümesindeki parçalar yerleştirilir. Sonrasında en alt seviyeden yukarıya doğru ikili bir şekilde özetleme değeri üretilerek ilerlenip, tüm ağaç yapısı için tekil bir özetleme değeri (Merkle kök değeri) üretilmiş olur. [1]



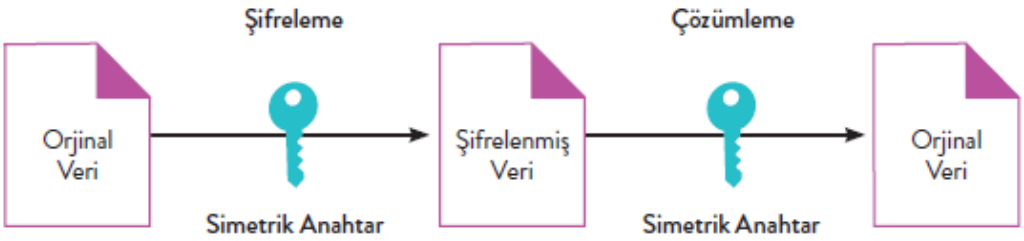
Şekil 4: Merkle Ağaçları

Kaynak: Blockchain 101

Şifrelenecek veri kümesi ve bir anahtar veri yapısı ile şifreleme işlemi yapılmaktadır. Şifreleme işlemi 2 farklı yöntemle yapılmaktadır.

2.8.1. Simetrik Şifreleme

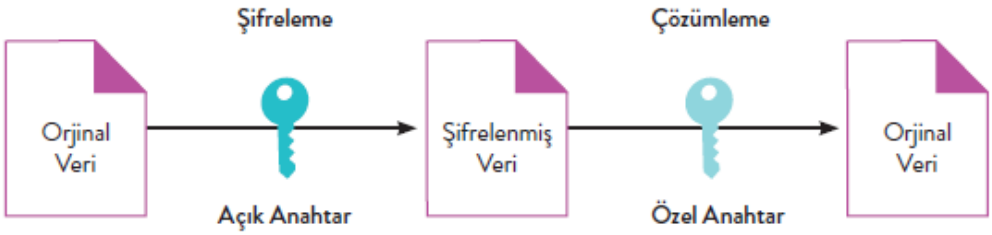
Bu yaklaşımda hem şifreleme hem çözümleme adımlarında aynı anahtar bilgisi kullanılmaktadır. Bundan dolayı anahtar bilgisinin sadece ilgili taraflar arasında paylaşılması gerekmektedir. Anahtarı ele geçiren herhangi bir taraf şifrelenmiş veriden orijinal veriye erişebilir. [1]



Şekil 5: Simetrik Şifreleme
Kaynak: Blockchain 101

2.8.2. Asimetrik Şifreleme

Bu yaklaşımda şifreleyen ve çözümleyen anahtar bilgileri farklıdır. Temel olarak bu yöntem içerisinde kullanıcının biri herkese açık (public) diğeri ise sadece kendi içerisinde saklı tuttuğu özel (private) anahtar çifti değeri bulunmaktadır. Bu açık anahtar herkese dağıtılabilir. Açık anahtardan özel anahtara ulaşmak, bunun için gerek duyulan çok yüksek hesap gücünden dolayı imkânsız olarak nitelenmektedir. Ayrıca açık anahtar ile şifrelenmiş bir veri, ancak ilgili özel anahtar ile çözümlenebilmektedir. Benzer şekilde özel anahtar ile şifrelenmiş veri de ancak ilgili açık anahtar ile çözümlenebilmektedir. [1]



Şekil 6: Asimetrik Şifreleme
Kaynak: Blockchain 101

2.9. Mutabakat Yapısı

Mutabakat adı verilen kurallarla Blokzincir ağındaki verinin bir kopyasının ağda yer alan tüm makinelerde yer alması, veri tabanında hangi değişikliklerin yapılmasına izin verildiği ve bu değişikliklerin kimler tarafından yapılabileceğine karar verilir. Tezimizde, Proof of Work (PoW) ve Proof of Stake (PoS) protokollerine yer vereceğiz.

2.9.1. Proof of Work (PoW)

Bu yapıda sistemin bir blok yapısı hazırlanıp ilgili Blokzincir ağına eklenmesinin yönetimi için çözülmesi zor ama çözümün doğruluğunun kolay kontrol edildiği bir problem üzerinden ilerlenir. Bu konuda en çok kullanılan problem türü, hazırlanan bloğa ait özetleme (hash) değerinin belirli bir yapıya (tanımlanmış bir değer aralığı içerisinde olma, belirli bir karakter dizisi ile başlama gibi) uymasıdır. Özetleme (hash) fonksiyonları yapı itibari ile tek yönlü olduklarından ve çıktıları tahmin edilemediğinden, uygun bir değer üretilmesi için oldukça fazla sayıda deneme yapılması gerekmektedir. Şu andaki en popüler Blokzincir platformu olan Bitcoin üzerinde bu mutabakat yaklaşımı kullanılmakta ve ilgili süreç madencilik (mining) olarak adlandırılmaktadır. [1]

2.9.2. Proof of Stake (PoS)

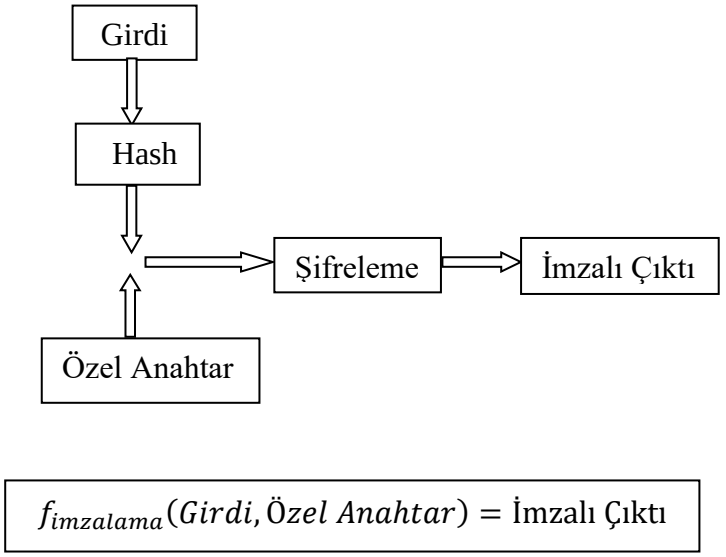
Proof Of Stake, PoW gibi bir mutabakat altyapısıdır. PoS protokolünde, sistemde üretilebilecek olan tüm kripto paralar başlangıçta üretilip üyeler yatırımları oranında kripto para sahibi olurlar. Blok üretimi ve onay mekanizması blok üretimi gerçekleştiren düğümün Blokzincir ağı üzerinde sahip olduğu pay ile doğru orantılıdır. PoW' da gücünüzü artırabilmeniz için madencilik yaptığınız cihazların sayısını ya da gücünü artırmanız gerekmektedir. PoS' ta ise sistemde sahip olduğunuz kripto para oranını yükseltmelisiniz. PoS protokolünde bir sonraki bloğu üretecek olan makinenin öncelikle sistemdeki payına bakılır ve payı yüksek olan seçilir. Eğer seçilen makine uygun bir süre içerisinde blok üretimini gerçekleştiremez ise bir sonraki makineye geçilir. Yüksek pay sahibi makinelerin sürekli olarak ilk üretim önceliğine sahip olmalarını düzenlemek adına yaş (age) kavramı geliştirilmiştir. Böylece blok üretimi için kullanılan pay kapsamındaki kripto paraların yaş (age) değerleri sıfırlanır ve bu paralar ancak bir süre sonunda yaş (age) almaya başlarlar. Yaklaşım kapsamında blok üretim süreci para basma olarak ifade edilmektedir. [8]

Ethereum' un PoS test ağı Mart 2019' da başlatılmış olup 2019 yılı bitmeden Ethereum platformu üzerinde Proof of Stake mutabakat yaklaşımının kullanılması hedeflenmektedir. Proof Of Work, fazla enerji tüketmekte olup pahalı bir mutabakatken; Proof Of Stake, blok oluşturma ve işlemlerin doğrulanma süresini kısaltmaktadır.

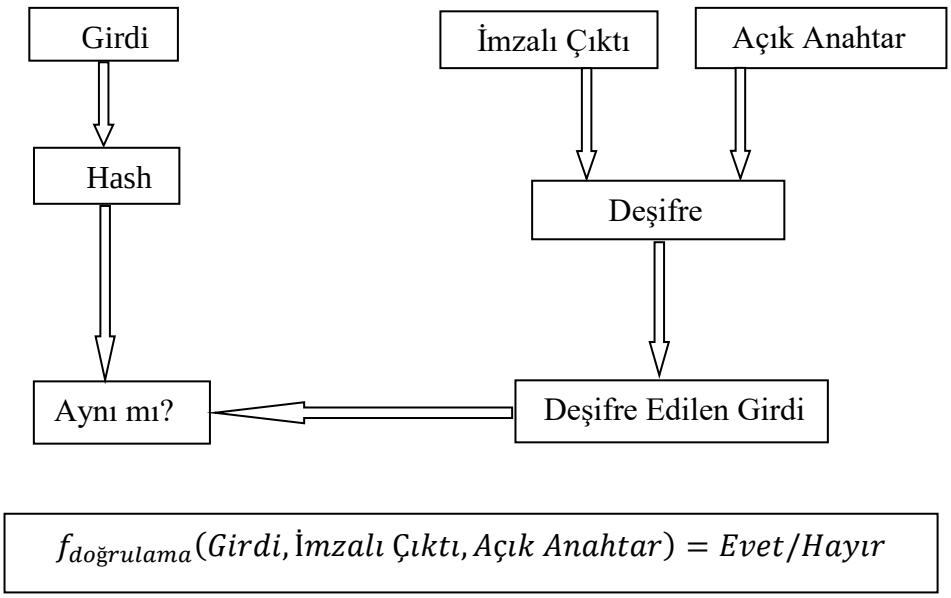
2.10. Dijital İmza

Dijital imza, açık (public) ve özel (private) anahtar ikilisiyle çalışan, matematiksel olarak güvenirliği ispatlanmış şifreleme yöntemidir. Dijital imza atmak isteyen herkesin kendine ait özel ve açık anahtarı olması gereklidir. Özel anahtarla şifrelenen bir girdi, sadece şifreleyene ait açık anahtarla çözülebilir. Özel anahtar sadece imzalayanda bulunur, kimseyle paylaşılmaması gerekir. Açık anahtarın dağıtılmasında mahsur yoktur. Özel anahtarla yapılan şifreleme işlemine imzalama denir. [9]

Girdiyi gönderen kişi, girdi ve imzalı çıktıyı karşı tarafa gönderir. Alıcı, göndericinin açık anahtarı ile imzalı çıktıyı deşifre eder. Deşifre edilen imzalı çıktı, alınan çıktı ile aynı ise girdinin kesinlikle gönderici tarafından imzalanmış olduğu ortaya çıkar. Girdide küçük bir değişiklik yapılmış olursa, deşifre edilmiş çıktı ile alınan çıktı birbirine uymayacaktır. Artık girdiyi imzalayan kişinin kimliği doğrulanmıştır ve girdinin hiçbir şekilde değiştirilmediği de kesindir.



Şekil 7: İmzalama



Şekil 8: Doğrulama

Açık anahtar, geri dönüşü olmayan eliptik eğri çarpımı kullanılarak özel anahtardan hesaplanır. K = k * G eşitliğinde k özel anahtardır. G, jeneratör noktası adı verilen sabit bir noktadır ve K sonuç olarak ortaya çıkan açık anahtardır. Daha açık olarak, özel anahtardan açık anahtar elde edilebilir ancak açık anahtardan özel anahtarı bulmak mümkün değildir. [10]

256 adet ardışık 0 veya 1'le, $2^{256} \approx 1.15 \times 10^{77}$ farklı gizli anahtar üretilebilmektedir. Gizli anahtar üretmek, 1 ile 2^{256} arasında rastgele bir tam sayı üretmek olarak da görülebilir. Herhangi iki farklı kişinin gizli anahtarının aynı olma ihtimali (çarpışma), yaklaşık 10^{77} de 1' dir. 10^{77} çok büyük bir rakamdır. Gözlemlenebilen evrende $\approx 10^{80}$ atom olduğu düşünülmektedir. Eğer açık anahtardan gizli anahtar elde ediliyor olsaydı sistem tamamen güvensiz olmuş olurdu. [9]

3. BLOKZİNCİR TEKNOLOJİSİ

İnternetin 90’ lı yıllarda bulunduğu yer ile günümüzdeki Blokzincir teknolojisinin bulunduğu yeri birbirine benzetmek mümkündür. Bu benzerlik yapısal bir benzerlik olmayıp gelecek yıllara etkileri yönünden bir benzerliktir. Bu benzetmeye odaklandığımız takdirde Blokzincir teknolojisinin 20 yıl içerisinde dünyanın dört bir tarafını etkisi altına alacağı ve dünyayı teknolojik olarak dönüştüreceği söylenebilir.

Blokzincir, işlem kayıtlarının tam listesini içeren, anlaşmaya dayalı bir blok dizisidir. [11]

Blokzincir teknolojisi, temel olarak bir kayıt teknolojisi olup yapılan işlemlerin kayıt edildiği, verilerin kolaylıkla izlendiği, paylaşıldığı dağıtık bir kayıt şeklidir.

Blokzincir teknolojisi, teyit görevi yapan üçüncü bir tarafa gerek duymadan birçok prosedürün gerçekleştirilebilmesini sağlamaktadır. Yapısal olarak bir blokzinciri, güvenli bir şekilde zincirlenmiş bir dizi bilgi bloğudur. Katılımcılar, yeni bilgi parçaları oluşturduğunda veya bir varlık hakkında mevcut bir bilgiyi değiştirdiklerinde yeni bloklar tanımlanmaktadır. İlk bloktan sonra yeni oluşturulmuş geçerli bloklar, güvenilen bir önceki bloğa güvenli bir şekilde zincirlenir. Böylece blokların güvenirliğini garanti ederek güvenilir bir denetim kanıtı oluşturulmaktadır. [7]

Teknolojinin en yaygın kullanıldığı alan finans alanı olup en çok bilineni kripto paralardır. Ancak kripto para konusuna dünya ülkelerinin yaklaşımı farklıdır ve bu sebeple kripto paraların kanuni statüsü farklılık göstermektedir. Dünyada olduğu gibi ülkemizde de kripto para olan Bitcoin ile ödeme kabul eden şirketler bulunmaktadır. Bilişim, eczane, eğitim, eğlence, emlak, E-Ticaret, ev dekorasyon, konaklama, hukuk, kırtasiye, reklam, teknoloji ve yayıncılık gibi birçok alanda yüzü aşkın sayıda Bitcoin kabul eden şirket bulunmaktadır.

Blokzincirin ilk özelliği kayıtların tek bir alan yerine eş zamanlı olarak farklı yerlerde kayıt edilmesidir. Bu kayıt sistemine "dağıtık defter" sistemi adı verilmektedir. Bu sayede, hem verinin tek bir sahibi olmamakta ve otorite paylaşılmakta hem de merkezi bir aracıya ihtiyaç duyulmamaktadır. İkinci olarak, tekil kayıtlar bloklar haline getirilirken kullanılan şifreleme yöntemi tek bir kaydı değiştirmek için bloklardan oluşan tüm zincirin değiştirilmesini zorunlu kılmakta, bu sayede dışarıdan müdahaleler mevcut işlemci teknolojileri ile neredeyse imkânsız hale gelmektedir. Bu özellikleriyle Blokzincir kayıtların güvenilirliği ve korunması hususlarında mevcut teknolojilerden daha az maliyetli ve verimli çözümler sunmaktadır. [12]

Dağıtık defter sisteminde, birden fazla taraf mevcut olup tarafların birbirini tanımadığı durumlar da göz önüne bulundurulursa sistemin herkes tarafından kabul edilen yasası olmalıdır. Dolayısıyla bu yasayı oluşturabilmek için tarafların bir mutabakat içinde olması gerekir.

Sınırlı sayıda birey bir araya geldiklerinde el sıkışarak sözlü veya yazılı bir kayıt ile bir mutabakat sağlayabilirler. Dijital bir sistem üzerinde mutabakat yapısının sağlanması için, bunun yazılım kodları kullanılarak garanti altına alınması gerekir. İşte tam bu noktada Blokzincir teknolojisi, baştan mutabakat yapısı (kuralları) belirlenmiş şekilde veriyi kaydetmemizi sağlar ve bu kayıtları iletişim ağları üzerinden pek çok noktaya dağıtır. Bu süreç içinde verinin tüm noktalarda aynı kaldığına dair güveni mutabakat süreci sağlar. Hatta tüm kullanıcıların verilerini şifreleyeceği bir çözüm de sunar. Bu noktada Blokzincir teknolojisi, dijital dünyada artık kolaylıkla oluşturulabilen, güncellenebilen ve silinebilen veri kullanım şekline farklı bir bakış açısı getirmektedir. Blokzincir teknolojisi dağıtık bir veri kayıt sistemi olup kaydedilen bir veri sonsuza kadar değiştirilemez. Böylece güvenilir bir yapı ortaya çıkar. [1]

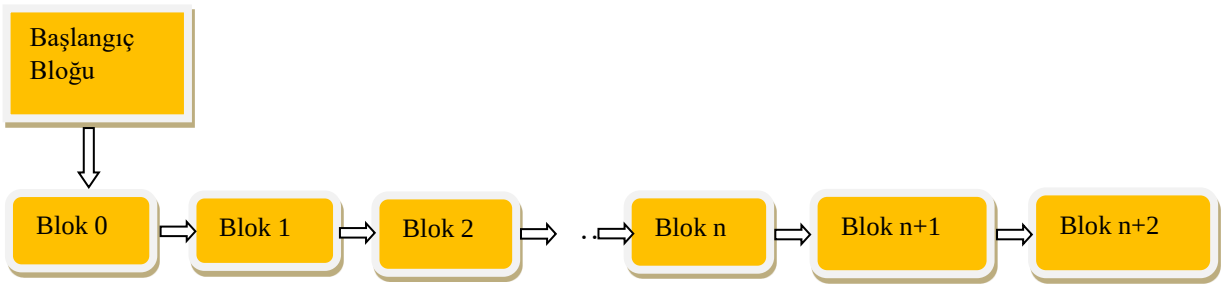
Şimdi Blokzincir teknolojisini birkaç örnekle açıklayalım.

Define aramak için yola çıkan 4 arkadaş amaçlarına ulaşmış ve aradıkları defineyi bulmuşlardır. Artık her birinin ganimet dolu birer küpü vardır. Küpler oldukça ağır olduğundan küpleri taşıyamamışlar ve küpleri güvenli bir yerde saklayıp daha sonra küpleri taşıyabilecekleri vasıta ile gelip almaya karar vermişlerdir. Ne zaman

gelip alacakları belli olmadığından hangi küpün kime ait olduğunu küplerin kapaklarının üzerine yazıp isimlerin altına da imzalarını atmışlar ve küpleri yan yana zincirlemişlerdir. Kişi isimleri ve imzalarını veri, küplerin her birini blok olarak düşünebiliriz.

Şekil 9: Küplerin blok düzeni

Böylelikle kendine ait imzaya sahip olan bloklar yan yana dizilerek bir Blokzinciri oluşturulmuş oldu. Burada ilk bloğa başlangıç bloğu adı verilir.

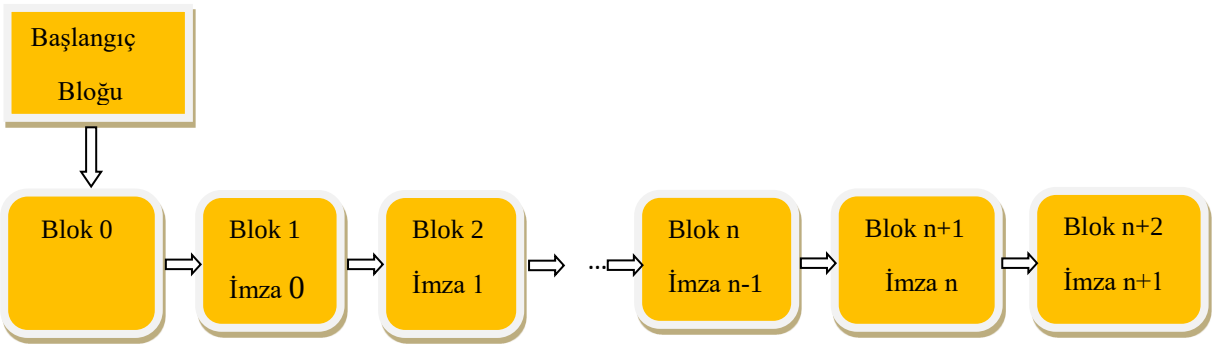


Şekil 10: Blokların birbirini takip etme düzeni

Ancak küplerin kapaklarını çıkarıp yerlerini değiştirmek mümkündür. Bu durumu düşünen 4 kişi, yeni bir mutabakat oluşturarak küplerin kapağına isim yazıp imza attıktan sonra başlangıç bloğu olarak düşündüğümüz küpten itibaren her küpün kapağına kendinden önceki küpün sahibi tarafından imza atılmasına karar vermiştir.

Şekil 11: Küplerin blok düzeni

Böylelikle küplerin kapaklarının yerleri değiştirilse bile kolaylıkla fark edilebilir duruma gelmiştir.



Şekil 12: Blokların, kendinden önceki bloğun dijital imzasını içerdiği takip düzeni

Başlangıç bloğu sadece kendisine ait imzayı taşırken sonraki bloklar hem kendisine hem de bir önceki bloğa ait imzayı taşır. Böylelikle sıralı bir yapı meydana gelir.

Definecilerin tedirginliği ortadan kalkmış gibi duruyor ancak atılan imzaların taklit edilme olasılığı göz ardı edilmemelidir. Bu sebeple, defineciler arasında yeni bir mutabakata ihtiyaç doğmuştur. Bu yeni mutabakata göre, küplerin kapağına isim yazıp imza attıktan sonra başlangıç bloğu olarak düşündüğümüz küpten itibaren her küpün kapağına kendinden önceki küpün sahibi tarafından imza atılması sonucunda ele edilen zincir örneği, herkes için birer kopya yapılarak definecilere dağıtılacaktır.

Ali ECE’ nin kopyası

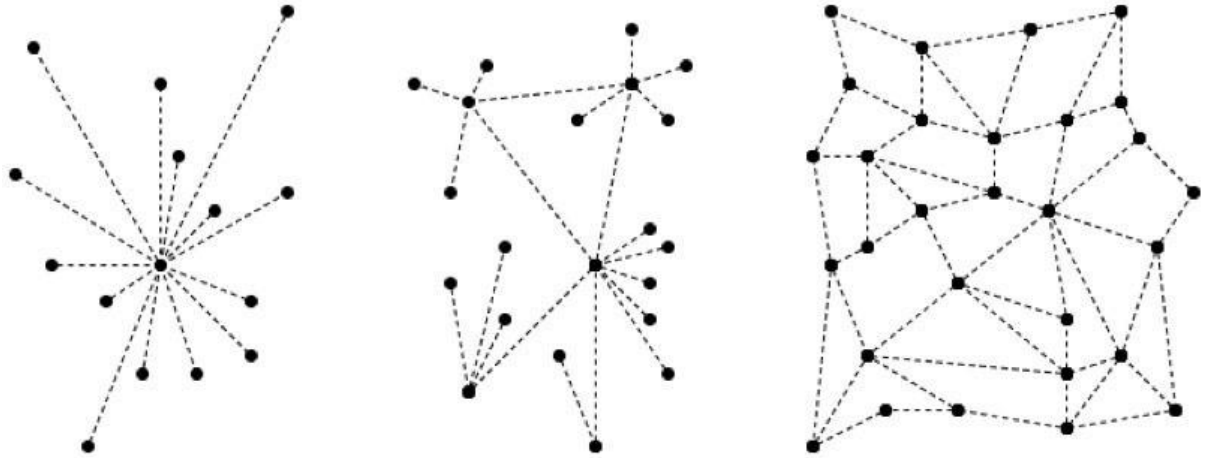
Kaya ÖZ’ ün kopyası

Alp METE’ nin kopyası

Can KARA’ nın kopyası

Şekil 13: Küplerin blok düzeni

Artık herkesin onayıyla oluşturulan mutabakata göre hayata geçirilen zincirin herkeste birer örneği mevcuttur. Herkeste birer örneği olan zincirde herhangi bir kişinin yapabileceği değişiklik anlamsız olacaktır. Çünkü herkeste kopyası bulunan zincir örnekleri birbiri ile karşılaştırılıp yapılan hile ortaya çıkarılacaktır. Bu durum ise oluşturulan sisteme olan güveni sağlayacaktır.



TEK MERKEZLİ AĞ **ÇOK MERKEZLİ AĞ** **DAĞITIK AĞ**

Şekil 14: Ağ yapıları

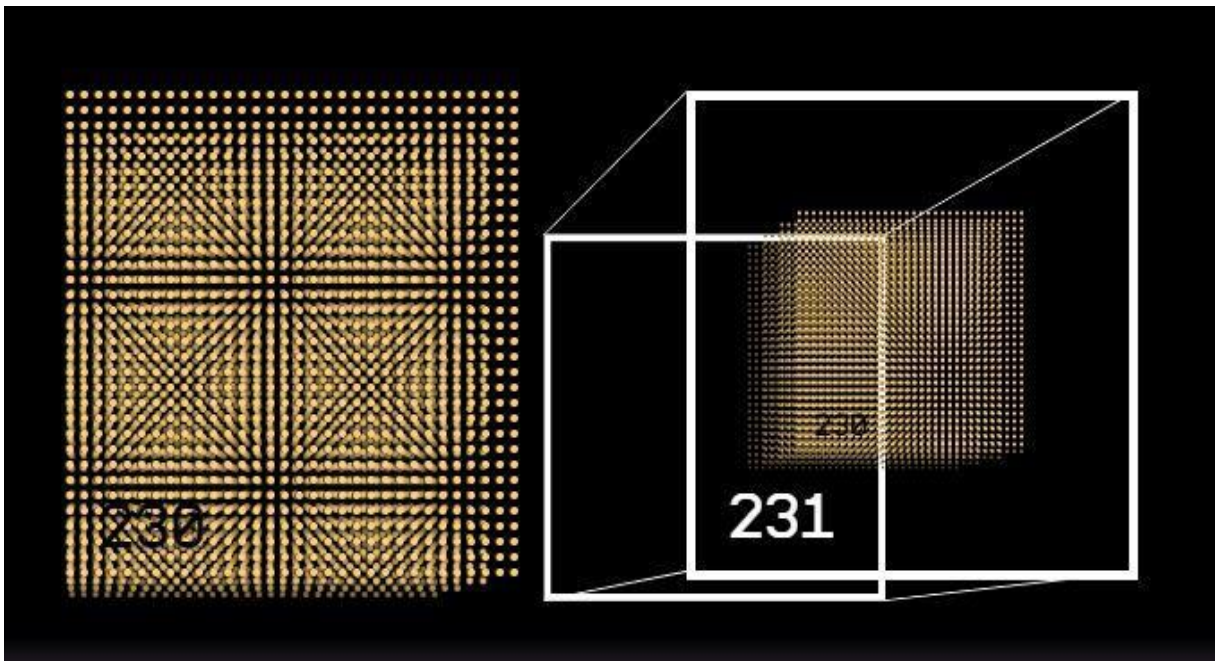
Blokzincir teknolojisinin insanlığa sunduğu, tam olarak örnekte anlattığımız yapıdır. Bu teknolojide veri sadece bir merkez tarafından değil, sisteme dâhil olan tarafların tamamı tarafından kayıt edilmektedir. Blokzincir teknolojisinde taraflar birbirini tanımak ve birbirine güvenmek zorunda olmayıp sisteme güven esastır. Çünkü mutabakatla oluşturulan sistemin belirlenen kurallar çerçevesinde oluşturulan kayıtları herkeste bulunmaktadır. Söz konusu kayıtların dağıtıldığı taraflar, sürekli iletişim halindedir ve zincir yapısında herhangi bir değişiklik olması durumunda hemen yeni mutabakat oluşturularak sistem kullanılmaya devam edilir.

Blokzincir teknolojisiyle ilgili biraz daha detaya girelim.

Bu kayıt sisteminde, Blokzincir ağına bağlı kullanıcıların (her bir kullanıcıya düğüm (node) ismi verilmektedir) kaydettikleri veriler (örneğin, yapılan bir alışveriş) tüm ağa dağıtık şekilde yayılmaktadır. Ağa yayılan belli sayıda işlem üzerindeki zaman damgası ile birlikte bir veri bloğu haline getirilmektedir. [12]

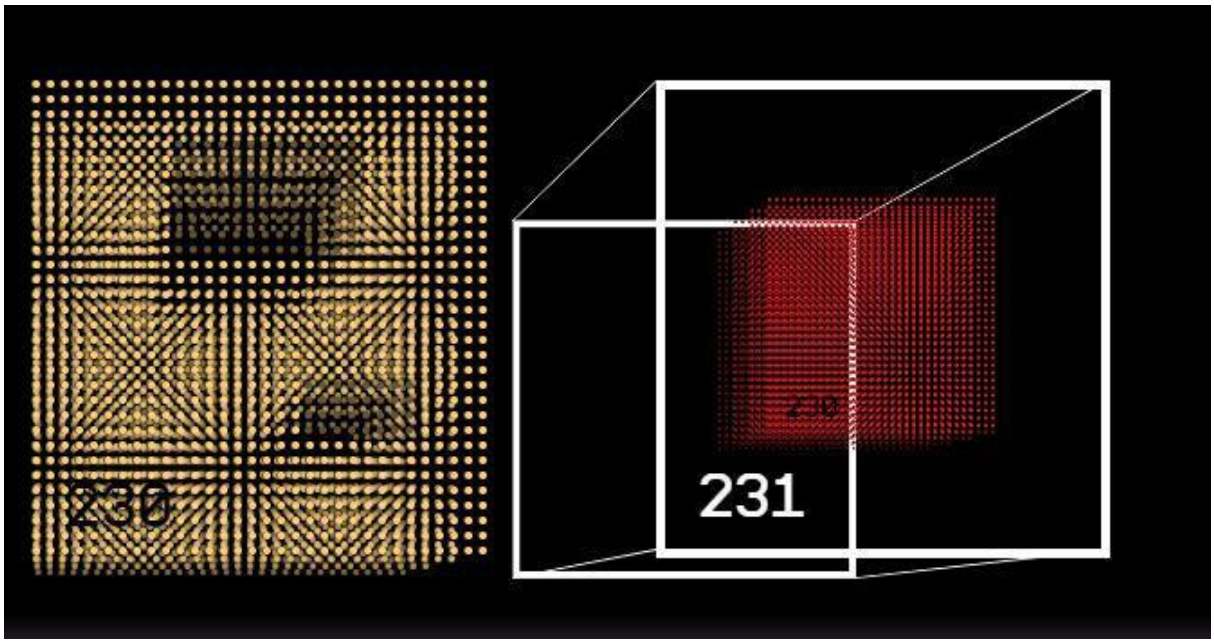
Bahse konu edilen bloğu ilk oluşturan olmak için rekabet halinde olan şirket ve kurumlar, oluşturdukları ilk blok için benzeri olmayan bir kod oluşturmaktadırlar. Bir blokta, veriler ve blok başlığı olmak üzere iki temel kısım bulunmaktadır.

Bir blok başlığı temel olarak bir önceki bloğa ait özetleme (hash) değeri, blokta yer alan verilere ait Merkle kök değeri ve zaman bilgisinin ihtiva eder. Bahse konu ettiğimiz blok yapısını aşağıdaki şekil ile gösterecek olursak, 231 numaralı bloğun içerisinde 230 numaralı bloğa ilişkin özet bilgi yer almaktadır



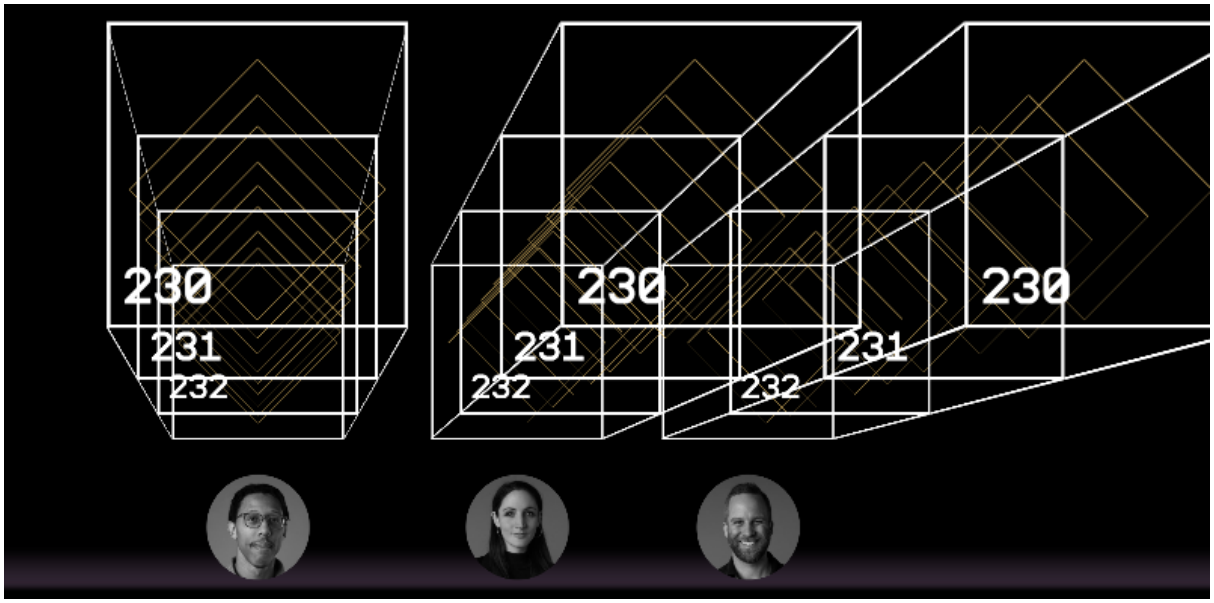
Şekil 15: Blok yapısı
Kaynak: Blokzincir Uygulamalarına İlişkin Kavramsal Çerçeve, Ticaret Bakanlığı

230 numaralı blokta herhangi bir değişiklik olduğunda söz konusu özet bilgi de değişmektedir. Bu durumda, 231 numaralı blokta yer alan özet bilgi ile tutarsızlık meydana gelmekte olup ve değişiklik yapıldığı anlaşılmaktadır.



Şekil 16: Tutarsızlık durumunda blok yapısı
Kaynak: Blokzincir Uygulamalarına İlişkin Kavramsal Çerçeve, Ticaret Bakanlığı

Blokzincir teknolojisi, blokların arka arkaya dizilerek oluşturduğu zincir mantığına göre çalışmakta olup bu zincir dağıtık ağda yer alan kullanıcıların tamamı ile paylaşılmaktadır.

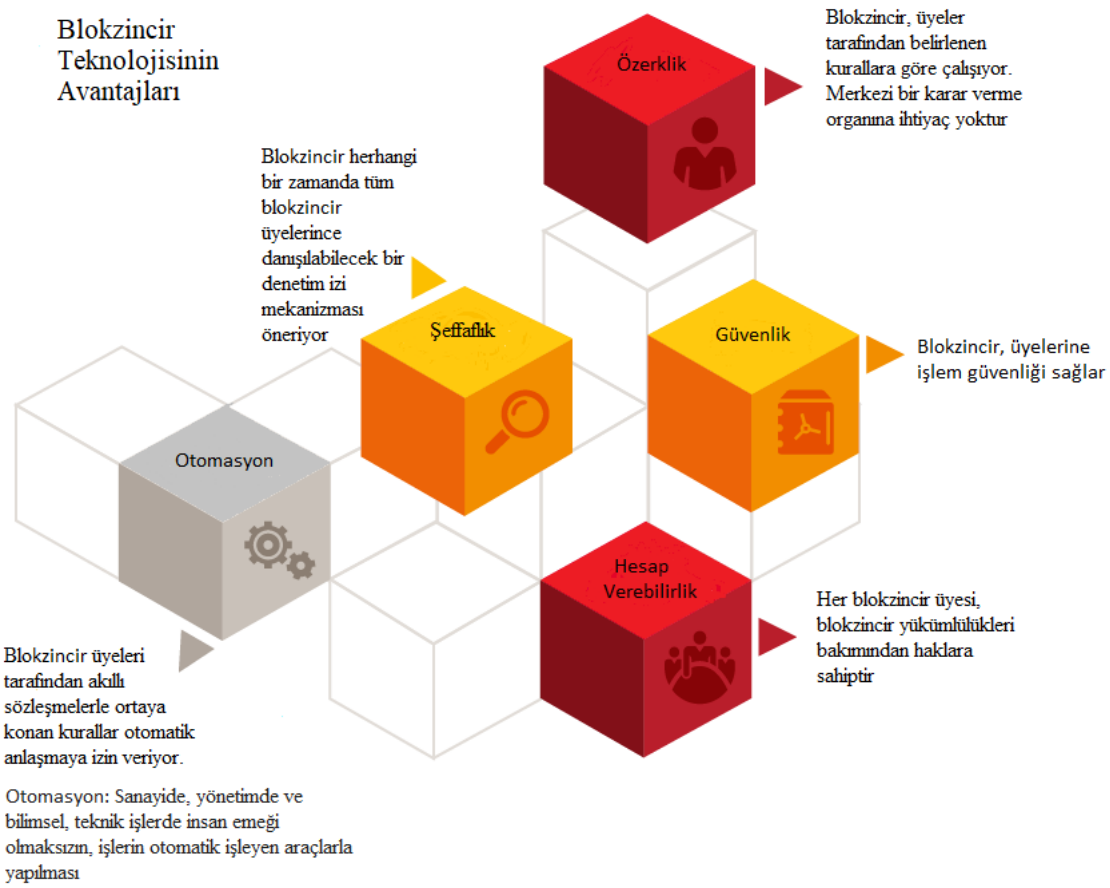


Şekil 17: Dağıtık ağdaki kullanıcıların tamamındaki zincir
Kaynak: Blokzincir Uygulamalarına İlişkin Kavramsal Çerçeve, Ticaret Bakanlığı

Şekilde görüldüğü gibi tüm kullanıcıların, kullandıkları dijital ortamlarında aynı blok dizilimine sahip zincirler bulunmaktadır. Söz konusu zincir üzerinde yer alan

herhangi bir blokta değişiklik yapmak için, değişiklik yapılan bloktan sonraki bütün bloklar değiştirilerek bütün kullanıcılarla paylaşılmalıdır. Ancak zincirde değişiklik yapmak kolay bir işlem değildir. Bu işlem yüksek işlem gücü ve ağda bulunan kullanıcıların yarısından bir fazlasının ortak kararı ile yapılabilir. [12]

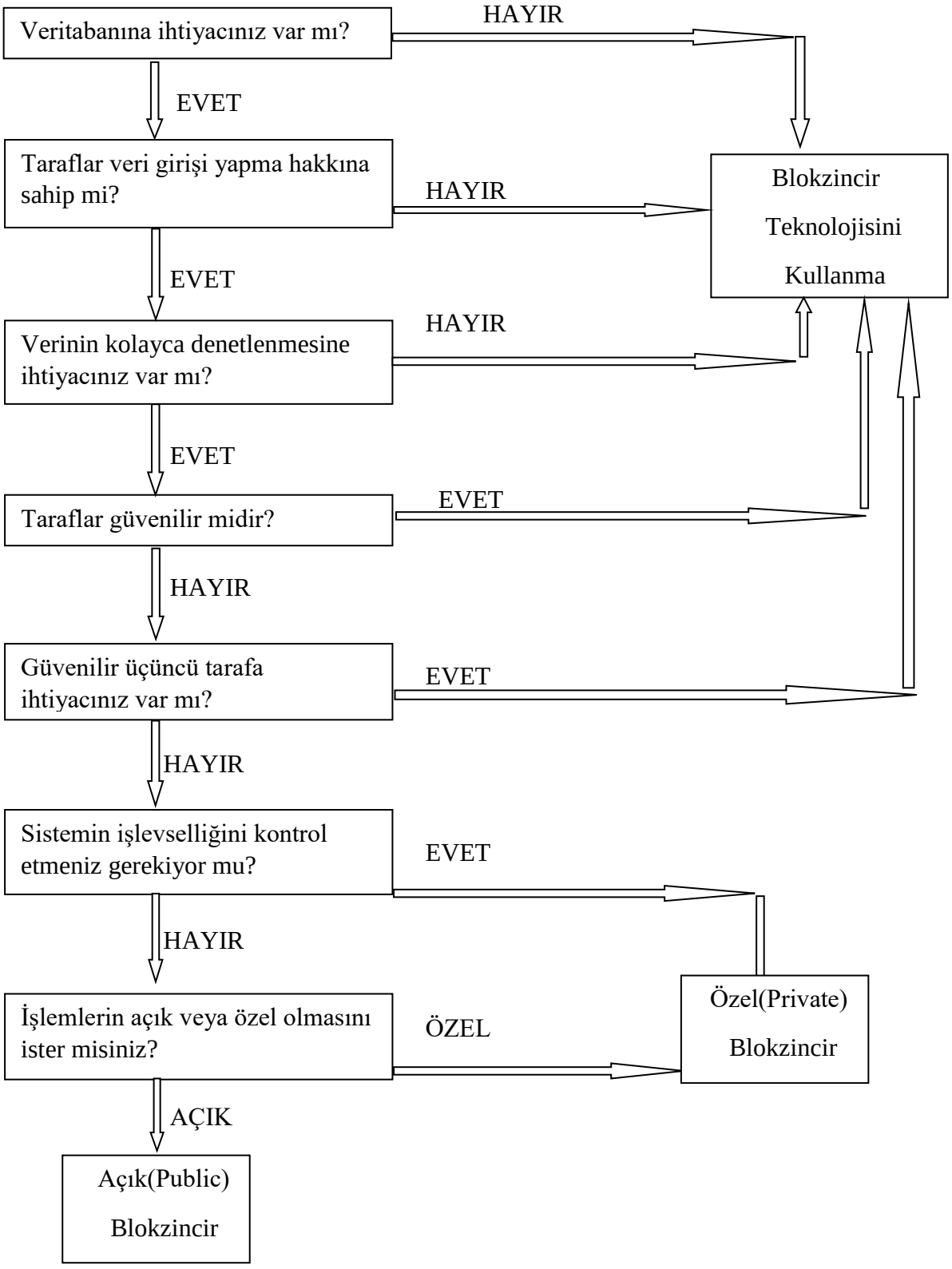
Güven merkezli ve değiştirilemez yapıda olan Blokzincir teknolojisi, birçok avantajı da beraberinde getirmektedir. Bu avantajlardan birkaçı aşağıdaki şekilde ifade edilmiştir.



Şekil 18: Blokzincir teknolojisinin avantajları

Kaynak: PwC France

Blokzincir teknolojisini kullanıp kullanmama konusunda karar vermeden önce bazı koşulların göz önünde bulundurulması gereklidir. Aşağıdaki tabloda, Blokzincir teknolojisi hangi koşullar oluşunca kullanılmalıdır sorusunun cevabı yer almaktadır.



Şekil 19: Blokzincir teknolojisi kullanımı karar mekanizması

Blokzincir teknolojisi,

- Birden fazla taraf veri paylaşıyor mu?
- Birden fazla taraf veriyi güncelleyecek mi?
- Paylaşılan veriyi doğrulama zorunluluğu var mı?
- Verinin doğrulanması, maliyet ve karmaşıklık getiriyor mu?
- Etkileşimler zamana duyarlı mı?
- Farklı kullanıcılar tarafından yapılan işlemler birbirine bağlı mı?

sorularından en az 4 tanesine evet demeniz halinde sizin için bir çözüm olabilir.

3.1.Blokzincir Türleri

Blokzincir türlerini,

1- Açık (Public) Blokzincir Ağları
   a) Bütünüyle İzin Gerektirmeyen Blokzincir Ağları
   b) Kısmen İzin Gerektirmeyen Blokzincir Ağları
2-Özel (Private) Blokzincir Ağları
   a) Kısmen İzin Gerektiren Blokzincir Ağları
   b) Bütünüyle İzin Gerektiren Blokzincir Ağları

olarak sınıflandırabiliriz.

Şekil 20:Açık (Public) Blokzincir ağı

Kaynak: Pwc France

Şekil 21:Özel (Private) Blokzincir ağı

Kaynak: Pwc France

3.1.1. Açık (Public) Blokzincir Ağları

Herkese erişimin açık olduğu Blokzincir ağlarına verilen isimdir.

3.1.1.1.Bütünüyle izin gerektirmeyen blokzincir ağları

Bu tip Blokzincir ağlarındaki amaç, mümkün olan en çok sayıda kişinin ağa dâhil olarak zincirin kopyasına sahip olan kişi sayısının artması ile birlikte Blokzincir ağının daha güvenli hale gelmesini sağlamaktır. Eğer bir Blokzincir ağına girip ağda kayıtlı olan verilere ulaşmak ve zincire yeni bloklar ekleyebilmek için herhangi bir izin gerekmiyorsa bu tür ağlara "Bütünüyle İzin Gerektirmeyen Blokzincir ağları" adı verilir. Bütünüyle İzin Gerektirmeyen Blokzincir ağlarına verilebilecek en bilinen örnek Bitcoin' dir. Kullanıcılar, dijital ortama indirdikleri bir uygulama sayesinde Bitcoin ağına dâhil olabilirler.

3.1.1.2.Kısmen izin gerektirmeyen blokzincir ağları

Eğer bir Blokzincir ağına girip kayıtlı olan verilere ulaşmak için izin gerekmeyip, zincire yeni bloklar ekleyebilmek için izin gerekiyorsa bu tür ağlara "Kısmen İzin Gerektirmeyen Blokzincir ağları" adı verilir. Bu Blokzincir ağını bir örnekle açıklayacak olursak; Ülkemizde yaygın olarak kullanılan bilgi paylaşım platformlarından olan internet sözlüklerini (örnek: ekşi sözlük vb.) bir Blokzincir ağı olarak düşünelim. Ağa giren herkes sözlüğe yazılan her bilgiyi okuyabilir ancak sisteme sadece izin verilen kişiler bilgi ekleyebilmektedir.

3.1.2. Özel (Private) Blokzincir Ağları

Blokzincir ağına girebilmek için izin gerektiren Blokzincir ağına verilen isimdir. Halka açık Blokzincir ağları üzerinde kayıt bulundurmayı tehlikeli bulan şirketler ve kurumlar, ağa giriş yapabilmek için mutlaka izin alınması gerektiğini düşünmektedir. Özel bir blokzinciri kurmadan önce bir veri tabanının, ihtiyaçlarınız için daha uygun olup olmadığını sorgulamanız gereklidir.

3.1.2.1.Kısmen izin gerektiren blokzincir ağları

Eğer bir Blokzincir ağına girip kayıtlı olan verilere ulaşmak için ve zincire yeni bloklar ekleyebilmek için izin gerekiyorsa bu tür ağlara "Kısmen İzin Gerektiren Blokzincir Ağları" adı verilir. BİLGE sistemi bu ağ için uygun örnektir. Kullanıcı adı ve şifre sahibi olan kişiler BİLGE sistemine giriş yapabilir, kullanıcıların sistemi kullanarak oluşturduğu beyannamelere ilişkin bilgiler de Blokzincir ağındaki bloklara kaydedilir.

3.1.2.2.Bütünüyle izin gerektiren blokzincir ağları

Blokzincir ağına girip kayıtlı olan verilere ulaşmak için izin almak gerekiyorsa ve zincire yeni bloklar ekleyebilmek için izin tekrardan izin almak gerekmiyorsa bu tür ağlara "Bütünüyle İzin Gerektiren Blokzincir Ağları" adı verilir. Bütünüyle izin gerektiren Blokzincir ağlarında, kaydedilen verilere sadece konunun ilgilisinin ulaşmasına izin verilmektedir.

Bankalar arasındaki EFT işlemleri bu tür ağlara örnek olarak verilebilir. Bir EFT işlemi için tüm bankaların ortak bir Blokzincir ağının olduğunu varsayalım. Bu sisteme sadece bankalar girebilecektir. Bu ağda A bankasından B bankasına bir EFT işlemi gerçekleştiğinde bu işleme ait veriye gerektiği takdirde sisteme dâhil olan tüm izinli bankalar ulaşabilecekken ilgili işlemin sadece A ve B bankası tarafından yapılmasına izin verilmiştir. [1]

4. PARA BİRİMİ YAPILARI VE FİNANSAL TEKNOLOJİ

4.1.Paranın Tarihi

İnsanlık, mal ve hizmet ihtiyacını karşılarken ilk önce takas yöntemi, sonrasında sırasıyla emtia para, altın ve gümüş gibi değerli taşlar, altın karşılığı olan değerli kâğıtlar, altın karşılığı olmayan ancak güvene dayanan itibari para ve son olarak dijital ve sanal paralara doğru yönlenmektedir. Görülen o ki; para, bilimsel gelişmelere paralel olarak her geçen gün daha da soyutlaşmaktadır.

Bir ekonomide genel kabul gören değişim aracı, değer koruma aracı ve hesap birimi işlevlerine sahip olan varlık "para" olarak adlandırılmaktadır.

"Bir şeyin para olarak kabul edilebilmesi için aşağıdaki üç fonksiyonu sağlaması gerekmektedir.

- Mübadele aracı olma özelliği; bir ürün/hizmet alımı karşılığında paranın alıcı tarafından satıcıya verilebilmesidir.

- Ölçü birimi olma özelliği; paranın ürün, hizmet ve diğer işlemlerin piyasa değerinin ölçülmesinde kullanılan standart sayısal bir birim olması nedeniyle değer ölçebilmesidir.

-Değer saklama aracı olma özelliği; değerinin zaman içerisinde sabit seyretmesi sayesinde paranın tasarruf aracı olarak kullanılabilmesidir. Bugün harcanmayacak olan paranın biriktirilmesi halinde harcama gücü sonraya aktarılmış olur." [13]

Kâğıt para icat edilmeden önce çeşitli deniz kabukları, altın ve gümüş sikkeler değişim aracı olarak kullanılmaktaydı. Zaman içerisinde madeni paranın saklanması, taşınması zahmetli bir hal alırken güvenlik sorunu da oluşmaya başladı. Bu sebeplerden ötürü büyük ticaret erbapları üzerinde yazılar olan ve değer ifade eden, günümüzdeki senet benzeri kâğıtlar kullanmaya başladılar. Bu senetler kâğıt paranın ilk formu olarak görülmektedir.

Değişim aracı olan bu senetler, ilk olarak 600'lü yıllarda Çin' de kullanıldı. Banknot biçimindeki bu kâğıt paralar 1279 yılına kadar kullanılmaya devam etti. Matbaanın keşfi ile toplu olarak kâğıt basımı yapılmaya başlandı ve 13. Yüzyılın ikinci yarısından itibaren çok sayıda farklı para bir standarda kavuştu.

Tarihte bugünkü anlamıyla ilk banknot olan "Jiaozi", 1100' lerde Çin' de Song Hanedanlığı döneminde basılmış olup, altın paralarla birlikte kullanılmıştır. [14]

Şekil 22:Bilinen anlamda ilk banknot Jiaozi
Kaynak: www.citeco.fr (Erişim tarihi 22.07.2019)

En üstteki yuvarlaklar paranın mühürleri, orta kısımdaki yazılar madeni para cinsinden değeri, en aşağıda ise alışveriş resmedilmiştir.

Batıda ilk banknot 1661 yılında İsveç' te basıldı ve Avrupa kıtasında ilk resmi para tedavüle girmiş oldu.

Osmanlı İmparatorluğu'nda Sultan Abdülmecit tarafından 1840 yılında "Kaime-ı Nakdiye-ı Mutebere" adıyla, elle yapılmış ve her birinde resmi mühür yer alan kâğıt para basılmıştır. Ancak zaman içerisinde kaimelerin kolayca taklit edilmesi üzerine 1842 yılından itibaren matbaada basıma geçilmiştir.

1821 yılında ilk kez İngiltere' de altın standardı uygulamasına geçildi. Altın standardı, standart para biriminin belirli bir ağırlıkta altın olarak kabul edildiği para sistemidir. Altın standardında ya altın sikkeler yasal para olarak dolaşıma girer ya da kâğıt para istendiğinde sabit bir fiyatla altına çevrilebilir. Altın Standardı döneminde merkez bankaları, para birimi ve altın arasındaki resmi pariteyi (ülke para birimlerinin birbirine oranı) korumak zorunda idi. Bunu sağlayabilmek için merkez bankalarının yeterli miktarda altın bulundurması gerekirdi. Ödemeler dengesindeki açık veya fazlalık, merkez bankaları arasında altın sevki ile finanse edilmek zorunda olup klasik altın standardının uygulandığı dönemlerde döviz kurları ve fiyatlarda istikrar mevcuttu.

Paranın değerinin altın veya gümüş gibi kıymetli madenlere bağlanması ve para arzının hükümetin altın rezervleriyle sınırlandırılması olarak tanımlanan ve 1821'den itibaren uygulanan altın standardı birçok ekonomide 1920'li ve 1970'li yıllar arasında çökmüştür. Bunun gerçekleşmesindeki yan faktör dünya savaşlarının finanse edilmesi olmakla birlikte temel sebep dünyadaki altın rezervlerinin ekonomik büyümeye uyum sağlayamamasıdır. [13]

Altın standardının terk edilmesinden sonra II. Dünya Savaşı sırasında Temmuz 1944'te gerçekleştirilen Birleşmiş Milletler Para ve Finans Konferansında sadece ABD Dolarının altına ve diğer para birimlerinin de ABD Dolarına endekslendiği bir sistem olan Bretton Woods dönemi başlamıştır. [13]

Bretton Woods dönemi ile birlikte neredeyse bütün ekonomiler kâğıt parayı kullanmaya başlamış, teknolojideki ilerlemeye paralel olarak finansal piyasalar da

teknolojik hale gelmiş ve fiziksel olarak tutulan para hareketleri artık elektronik olarak banka hesaplarında tutulmaya başlanmıştır.

Yeni sistem, Uluslararası Para Fonu (IMF) ve Dünya Bankası'nın (WB) kurulmasına yol açmıştır. 1969 yılında Özel Çekme Hakkı (SDR, Special Drawing Right) çıkarılmıştır ve hala günümüzde kullanılmaktadır.

SDR, üye ülkelerin resmi rezervlerinin tamamlayıcısı olarak IMF tarafından oluşturulmuş uluslararası rezerv varlıklarıdır. Mart 2016 itibarıyla 204,1milyar SDR (yaklaşık 285 milyar dolar) ihraç edilmiş ve üyelere tahsis edilmiştir. SDR' ler, kullanılabilir para birimleri ile değiştirilebilmektedir. SDR' nin değeri, ABD Doları, Avro, Çin Renminbisi, Japon Yeni ve İngiliz Sterlini olmak üzere beş anapara biriminden oluşan bir sepete dayanmaktadır. [7]

4.2.Para Birimi Yapıları

4.2.1. Emtia Para

Değeri, yapıldığı üründen gelen paralara “emtia para” denir. Emtia paralar fiziksel varlıklardır. Dünya üzerinde farklı bölgelerde ve farklı zamanlarda, bakır, tuz, çay, inci, fildişi, sığır, demir, köle, sigara vb. emtia paralar bin yıllar boyunca para olarak kullanılmıştır. Tüm zaman ve mekânlarda en yaygın olarak kabul gören emtia para ise altın ve gümüş olmuştur. [9]

4.2.2. Temsili Para

İçinde belli oranda altın olan madeni paralar, altın fiyatının yükselmesi halinde birileri tarafından eritilerek, içindeki altının alınma riskiyle karşı karşıyadır. Kötü paranın iyi parayı kovması olarak da bilinen bu kanuna “Gresham kanunu” denir.

Para olarak doğrudan veya alaşımlı değerli metal kullanmanın pek çok zorluğu olduğundan, emtia para sistemi zaman içerisinde temsili para sistemine evrilmiştir. Altın ve gümüş tacirleri veya bankalar, karşılığında emtia para olan, istendiğinde emtia paraya çevrilebilen temsili paralar basmışlardır. Altına dayalı mali sistemde, yasal para

veya sertifika basanlar, bastıkları toplam değerin sabit bir oranda karşılığını altın/gümüş olarak tutarlar. [9]

4.2.3. İtibari Para

Kâğıdının taklit edilemeyeceği, merkezi otoriteye güven temelli, üzerinde yer alan imzaların ve yapıldığı kâğıdın taklit edilemeyeceği kâğıt paraya "itibari para" denir. İtibari paralar altın ve gümüşe dayalı değildir.

Altın standardının terk edilmesinden sonra 1944'te gerçekleştirilen Birleşmiş Milletler, Para ve Finans konferansında sadece ABD Dolarının altına ve diğer para birimlerinin de ABD Dolarına endekslendiği bir sistem olan Bretton Woods döneminin başladığından tezimizde bahsedilmişti. Yani, altına dönüştürülebilen tek para biriminin dolar olmasına, diğer para birimlerinin değerlerinin de dolara göre ayarlanmasına karar verilmiştir.

Amerika Birleşik Devletleri Başkanı Richard Nixon, 1971 yılında Amerikan Dolarının altın karşılığının bulundurulması zorunluluğunu kaldırmıştır. Günümüzde ülkelerin dolaşımda bulunan paralarının, altın karşılıklarının olma zorunluluğu yoktur.

4.2.4. Elektronik Para

6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun' da tanımlandığı üzere; Elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, bu kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değer.

Belirli bir fon karşılığında fiziksel olmayan sanal bakiyelerce piyasaya ihraç edilen, ödeme işlemlerini gerçekleştirmek için kullanılan, herkes tarafından da ödeme aracı olarak kabul edilen, devletlerin finansal denetim ve düzenleyici kurumlarının yükümlülüklerine bağlı parasal değerdir.

Kanada Merkez Bankasının tanımına göre; telefon, tablet, temassız kart, sabit disk veya sunucu üzerinde kişiler adına saklanıp, transfer edilebilen ancak yatırım amacıyla kullanılamayan sanal para birimidir. Örneğin; elektronik para kuruluşu olan bir cep telefonu operatörü ile cep telefonunuzu kullanarak ödeme yapabilirsiniz ve harcadığınız tutar faturanıza yansır.

Elektronik para, korunaklı bir teknolojik cihaz üzerinde saklanan parasal değerdir.

4.2.5. Dijital Para

Elektronik olarak saklanabilen ve transfer edilebilen paradır. Sadece elektronik olarak var olan bir ödeme aracı olup mal ve hizmet satın almak için kullanılır. Dijital paralar, elektronik olarak saklanan ve transfer edilebilen paralardır.

1980'lerin sonunda, Hollanda'da gece yarısı yakıt alan kamyon şoförlerini ve benzin istasyonlarını hırsızlığa karşı korumak için, akıllı kartlara para yüklenmesi ve bu paralarla yakıt alınabilmesi elektronik ödemenin ilk örneklerindendir. Yine o tarihlerde, Albert Heijn isimli bir perakendeci, müşterilerinin banka hesaplarından doğrudan ödeme yapabilmeleri için bankalara baskı yapıyordu. Bu baskı sonucunda, şimdilerde herkesin bildiği POS (Point Of Sale) cihazları ortaya çıktı. [9]

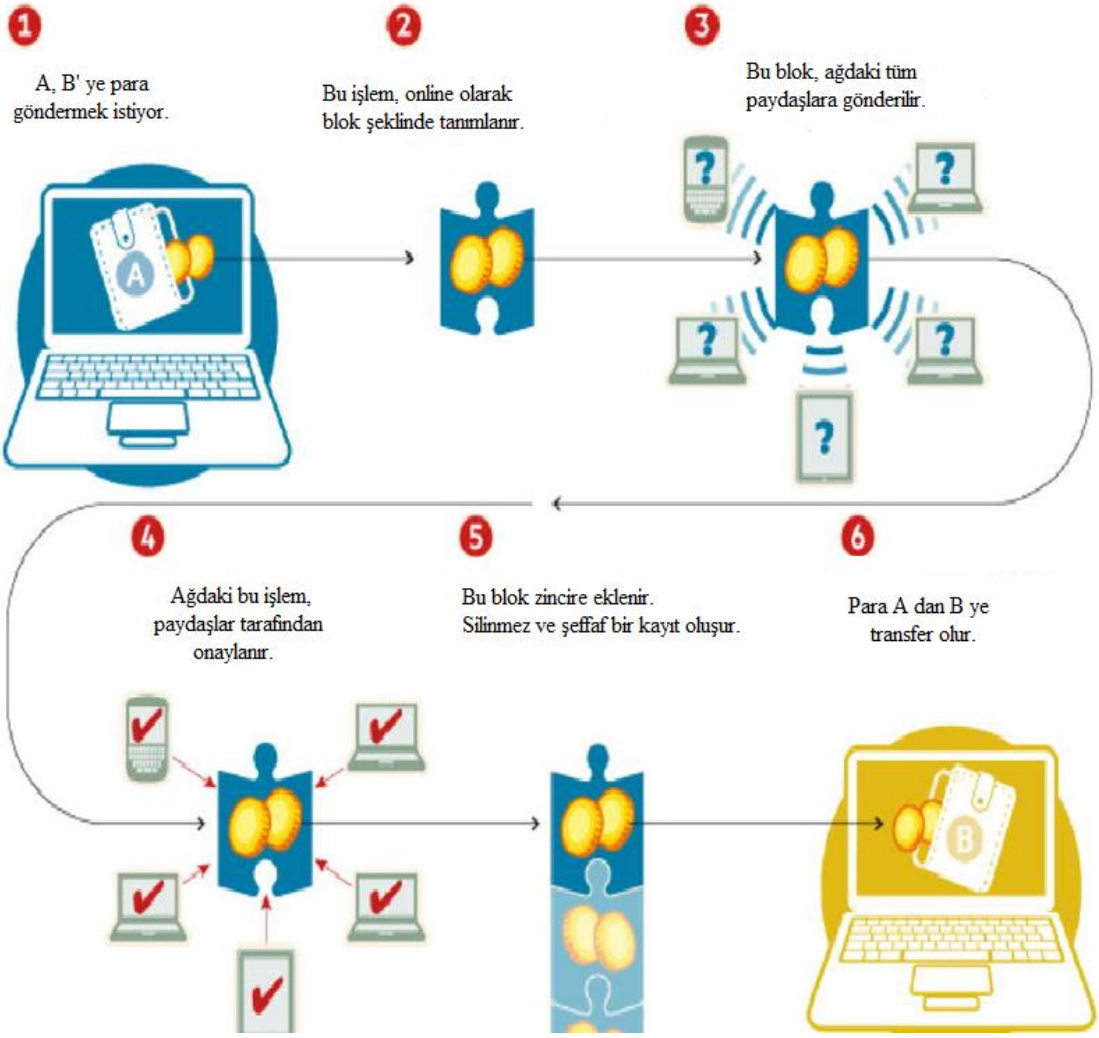
Fiziksel parayla yapılan işlemlerin oldukça azaldığı günümüzde, geleneksel para da dijitalleşmektedir. Dijital paraların saklanması ve transferi, merkezi olabildiği gibi dağıtık da olabilir. Merkezi dijital para işlemlerini, merkezi bir güç, otorite veya program denetler, gerçekleştirir. [9]

4.2.6. Kripto Para

Kriptolama teknikleriyle para birimlerinin oluşturulmasını düzenleyen ve (merkez bankasından bağımsız olarak işlem gören) fonların transferini doğrulayan bir dijital para birimidir. [7]

Sanal para arzına olanak sağlayan dijital değerlere kripto para denir. Kripto para, merkezi elektronik paraların ve bankacılık sistemlerindekinin aksine, merkezi olmayan yapıdadır. Kripto paralar hem dijitaldir hem de sanal paradır. Bitcoin ile dijital ve sanal paralar karıştırılmamalıdır. Bitcoin ve türevleri dışındaki dijital ve sanal paralar, temsil ettikleri ülkelerin ulusal para birimine endekslidir ve o ülkelerin merkezi otoritelerinin kontrolündedir. Bitcoin ise hiçbir otorite tarafından kontrol düzenlenip denetlenemez. Merkezi olmayan bu yapının kontrolü Blokzincir işlem veri tabanları tarafından gerçekleştirilir. [15]

Kripto paralar merkezi olmayan kripto sistemlerde, kamuya açık ve herkes tarafından bilinen yöntemlerle sistemin kuruluş aşamasında belirlenen oranlarda üretilir. Geleneksel para sistemlerinde hükümetler, gerekli gördüklerinde ulusal merkez bankaları aracılığıyla ek para ihraç edebilirler. Oysa hükümetler veya şirketler kripto para üretemezler ve başkalarının sahipliğindeki kripto paralara onların izni olmadan el koyamazlar. Dolaşıma sunulan kripto para miktarı ve para arzının şekli ve zamanlaması, kripto sistemin kuruluş aşamasında belirlenir. Kripto sistemlerde üçüncü bir taraf yoktur, güven gereksizdir. Güvenlik, bütünlük ve küresel hesap defterinin doğruluğu, karşılıklı birbirine güvenmeyen madenciler aracılığıyla gerçekleştirilir. Sistem güvenilirdir, ama taraflar birbirine güvenmezler. Kripto paranın güvenliği, madencilerin çoğunluğunun dürüstçe büyük defter tutma ve bundan finansal teşvik elde etme arzuları olduğu ilkesine dayanır. Çoğu kripto para sistemlerinde, dolaşımdaki toplam kripto paranın sabitlenebilmesi için kripto para üretimi zamanla azalmaktadır. Ülkelerin ihraç ettikleri dolaşımdaki banknot kağıt paralar itibari paralar olup, onları ihraç eden, denetleyen, düzenleyen bir otoritenin güvencesi altındadırlar. Buna karşılık, sanal kripto paralara olan güven, sanal para ihraç ve dolaşım sistemine ve sistem kullanıcılarının çoğunluğunun yanlış yapmayacağına olan inanç ile sağlanmaktadır. [9]



Şekil 23: Blokzincir teknolojisi ile para transferi

Kaynak: Berkeley, Applied İnnovation Review

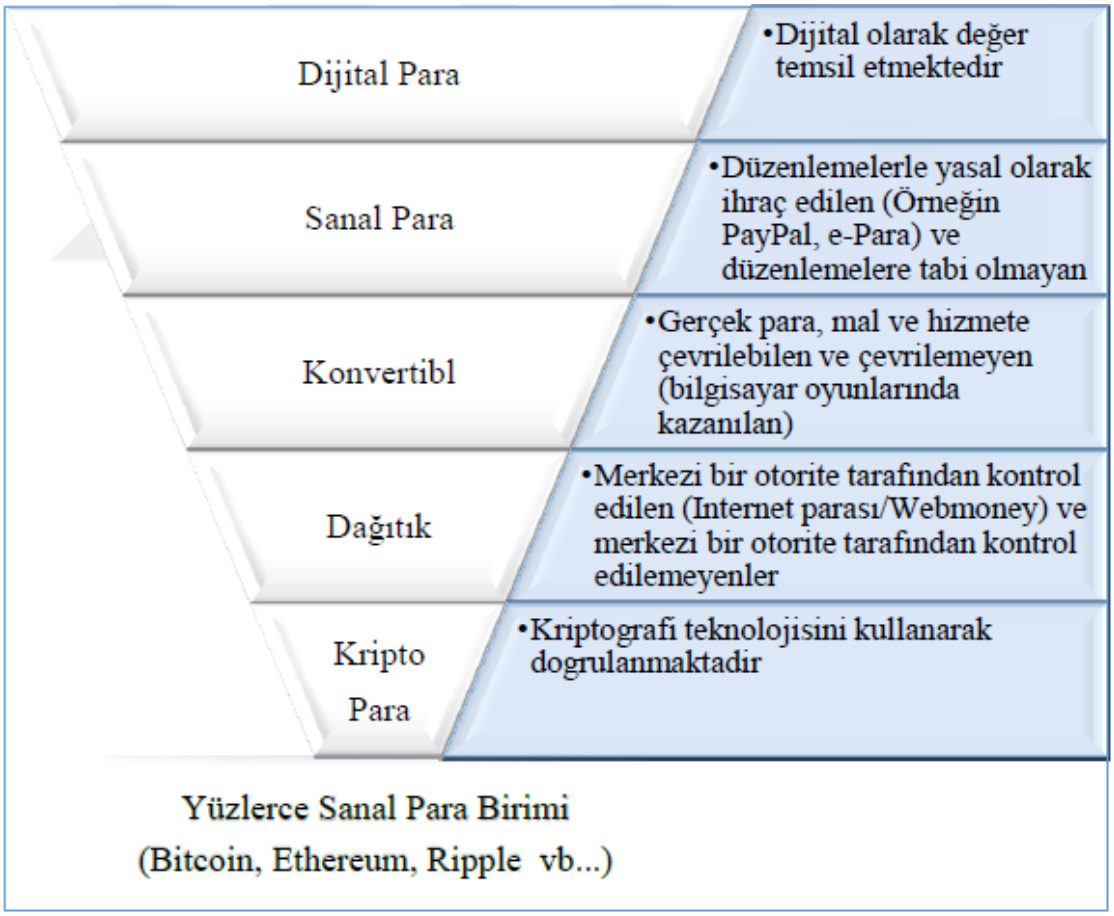
4.2.7. Sanal Para

Herhangi bir düzenlemeye tabi olmayan, ihracı ve kontrolü geliştiricileri tarafından yapılan ve genelde belli bir sanal topluluğun üyelerinin kendi aralarında çeşitli mal ve hizmetlerin değişiminde kullandığı sayısal para olarak tanımlanmaktadır. [16]

Avrupa Merkez Bankası 2015 yılında sanal parayı, "Herhangi bir merkez bankası, kredi kuruluşu ya da e-para kuruluşu tarafından ihraç edilmemiş, ve bazı durumlarda paraya alternatif olarak kullanılabilen varlığın sanal temsili" olarak tanımlamıştır.

Avrupa Bankacılık Otoritesi'ne göre, bir merkez bankası ya da kamu otoritesi tarafından arz edilmeyen ya da mutlaka bir emtia para birimine bağlı olmayan dijital bir değer gösterimidir. Sanal para birimleri doğal veya tüzel kişiler tarafından bir değişim aracı olarak kullanılmakta olup elektronik olarak aktarılabilir, depolanabilir veya ticareti yapılabilir.

Sanal paralar dijital paradır, ancak sanal paraların temsil ettikleri bir fiziksel gerçeklik yoktur. Sanal para dışındaki dijital paralar ise itibari kâğıt paraları temsil eder. [9]

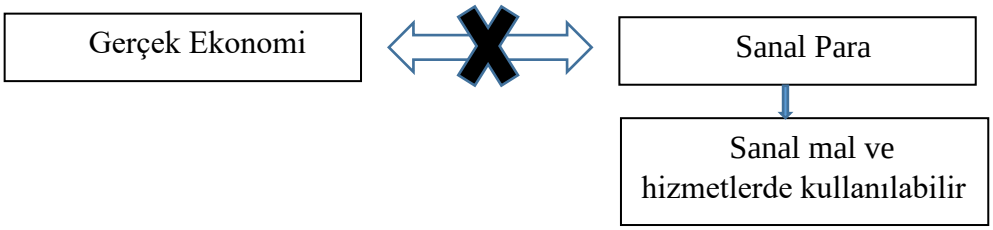


Şekil 24: IMF ye göre Sanal Para Birimlerinin Sınıflandırılması
Kaynak: Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları

Günümüzde çok sayıda sanal para birimi var olduğundan sanal para birimlerinin sınıflandırılması gerekmektedir. Bu sınıflandırma yapılırken sanal para biriminin diğer para birimleri ile değişim sürecindeki parasal akışa ve sanal para birimi ile gerçek mal ve hizmetler satın alınması sürecindeki akışa bakılabilir. Bu bakışa göre sanal para düzenekleri üçe ayrılır. [16]

4.2.7.1.Kapalı düzenekler

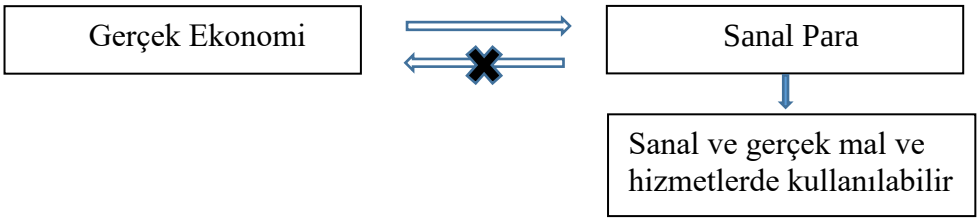
Gerçek Ekonomi ile bağlantısı olmayan düzeneklerdir. Bu düzeneklerdeki sanal paralar belirli bir sanal ortamdaki ürünler ve hizmetlerin satın alımında kullanılmaktadır. Örnek olarak, oyun sitelerinde kazanılan ve yine o oyun içerisinde harcanabilen paralar verilebilir.



Şekil 25: Kapalı düzenekler

4.2.7.2.Tek yönlü düzenekler

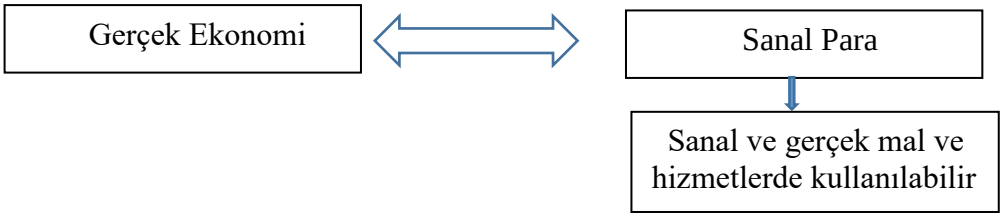
Bu düzenekte, itibari para birimi ile sanal para alınabilmekte ancak sanal para karşılığında itibari para alınamamaktadır. Bu düzenekteki sanal paralar ile sanal ve gerçek mal ve hizmet alınabilmektedir. Örnek olarak Facebook Credit verilebilir.



Şekil 26: Tek yönlü düzenekler

4.2.7.3.Çift yönlü düzenekler

Bu düzenekte kullanıcılar belirlenen kur çerçevesinde sanal para alıp satabilirler ve sanal paranın geçerli olduğu işletmelerden mal ve hizmet alabilirler. Örnek olarak Bitcoin verilebilir.



Şekil 27: Çift yönlü düzenekler

4.3. Finansal Teknoloji

Finansal hizmetlerin teknolojiyle buluşmasıyla ortaya çıkan finansal teknoloji durağan bir alan değildir. Bu alandaki aktörlere bakıldığında hepsinin zaman içinde birbirine dönüşebildiği görülmektedir. Örneğin finansal kuruluşlar giderek daha teknoloji odaklı bir yapı kazanmıştır. Büyük teknoloji şirketleri ise sosyal ağlar ve e-posta üzerinden eşler arası ödeme hizmetleri sunabilmektedir. Finansal teknoloji firmalarının sayıları her yıl artmakta olup en yoğun faaliyet perakende ödemeler alanında gösterilmektedir. [13]

Yenilikçi finansal teknoloji iş modelleri genellikle internet üzerinden otomatik olarak oluşturulan finansal ürün ya da hizmetlerin sunulmasını sağlamaktadır. Bu iş modelleriyle, bankalar ya da yatırım kuruluşları gibi geleneksel aktörler tarafından verilen hizmetler teknolojiye uyarlanmaktadır. Yapay zekâ, bilişsel bilim, makine öğrenimi ve Dağıtık Defter-i Kebir (DDK) gibi yeni teknolojiler ise hem finansal teknoloji alanına yeni giren şirketler hem de geleneksel finansal aktörler tarafından kullanıldığı için finansal hizmetleri dönüştürme potansiyeli taşımaktadır. [13]

Bankalar her ne kadar ödeme sistemleri ve kredi konularında tekel görevi görüyor olsa da finansal teknoloji şirketlerinin büyümesi ve 2008 yılında yaşanan bankacılık krizi sonrasında tüketicilerin bankalara olan güveni sarsılmıştır. Mobil cihaz kullanımının yaygınlaşması, finans teknoloji şirketlerinin mobil cihaz üzerinden hizmet sunması ve şeffaf ve erişim gücü yüksek veri tabanlarının dünya çapında artması ile birlikte finansal teknoloji şirketleri bankalarla rekabet konusunda başarı elde etmeye başlamışlardır.

Kripto para, finansal teknolojilerin son yıllarda ortaya çıkan en büyük teknolojilerinden biridir. Kripto para terimi ile finans dünyasının tanışması, Satoshi Nakamoto' nun "Bitcoin: A Peer-to-Peer Electronic Cash System" makalesi ile olmuştur.

5. BLOKZİNCİR PLATFORMLARI

İlk olarak finansal işlemler için kullanılan ancak zamanla diğer sektörlerce kullanılmaya başlayan Blokzincir teknolojisinin çalışma mantığını ve ağ yapısını detaylıca anlattığımız tezimizin bu kısmında Bitcoin, Ethereum (Akıllı Sözleşmeler), Hyperledger ve Ripple Blokzincir platformları hakkında bilgi verilecektir

5.1. Bitcoin

Bitcoin, Blokzincir kavramı ile tanışmamıza vesile olan temel platform olup aynı zamanda en çok bilinen ve tanınan Blokzincir platformudur. Kasım 2008'de Satoshi Nakamoto'nun "Bitcoin: A Peer-to-Peer Electronic Cash System" adlı makalesi ile ortaya çıkmıştır.

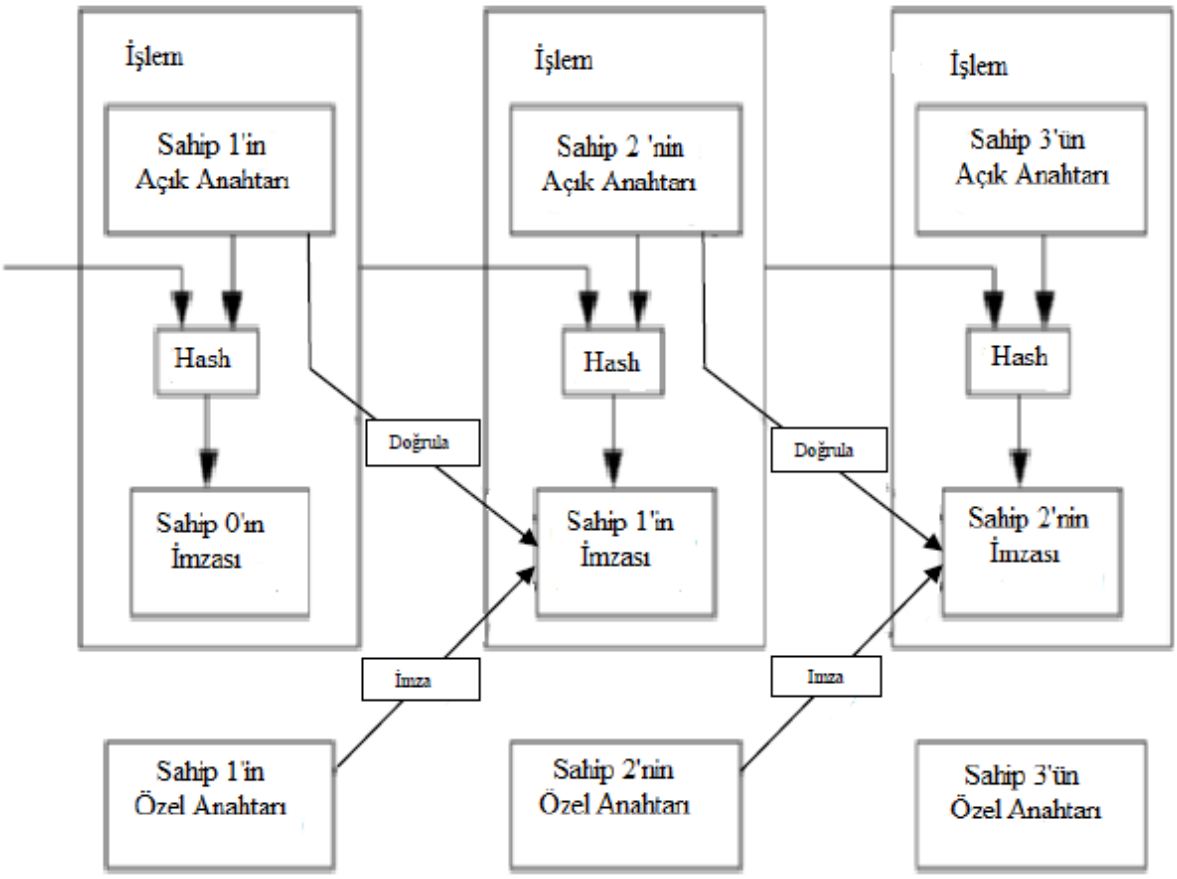
5.1.1. Bitcoin-Eşler Arası Elektronik Nakit Ödeme Sistemi

Günümüz dünyasında internet yoluyla yapılan alışverişlerde, taraflar ödeme için finans kuruluşlarına bağımlı haldedir. Ancak finans kuruluşlarıyla olan ilişki, güven esaslı olduğundan her an bozulma tehlikesiyle karşı karşıyadır. Finans kuruluşları, yaptıkları arabuluculuk karşılığında hizmet gideri almaktadır. Bu sebeplerden dolayı üçüncü tarafa ihtiyaç duymadan ödeme yapabilme ihtiyacı mevcuttur. İşte tam bu noktada, bu ihtiyacı giderecek kriptografi esaslı, üçüncü tarafa ihtiyaç duymayan, tarafların birbiriyle doğrudan işlem yapabileceği elektronik ödeme sistemine ihtiyaç duyulmaktadır. Bitcoin, uçtan uca para transferi ile bu sorunun çözümü için geliştirilmiş bir yaklaşımdır. Bu sistem, geri döndürülmesi imkânsız olduğundan tarafları koruyacaktır.

Bitcoin BTC, Bitcoin platformunun kripto para birimi olup platform üzerinden para transferi yapmak isteyen kişilerin dijital cüzdanları bulunmalıdır. Mevcutta pek çok mobil uygulama ve web sitesi gibi kanallar yardımıyla dijital cüzdan oluşturulabilir. Kullanıcılar için oluşturulan bu cüzdan ile cüzdan sahibi için bir adet açık bir adet özel anahtar oluşturulmaktadır. Açık anahtar transferler sırasında paylaşılabilirken özel anahtar saklı tutulmalıdır.

Bitcoin, elektronik parayı bir dijital imza zinciri olarak tanımlamaktadır. Paranın el değiştirmesi sırasında her sahip parayı sonrakine gönderirken kendi dijital imzasıyla bir önceki işlemin özetini(hash) ve bir sonraki sahibin açık anahtarını imzalar ve bu imzayı paranın sonuna ekler. Ödeme yapılan kişi sahiplik zincirini doğrulamak için imzaları doğrulayabilir. [17]

Elbette buradaki problem ödeme yapılan kişinin zincirdeki önceki sahiplerden birinin parayı iki kere harcamadığını doğrulayamamasıdır. Bu problemin yaygın çözümü, merkezi bir otoritenin her işlemin iki kere yapılıp yapılmadığını kontrol etmesidir. Her işlemden sonra para merkeze geri dönmelidir ve yeni bir para piyasaya sürülmelidir. Sadece otorite tarafından doğrudan piyasaya sürülen paraların mükerrer olarak harcanmadığına güvenilebilir. Bu çözümdeki sorun para sisteminin kaderinin her işlemin üzerinden geçtiği merkezi otoritenin elinde olmasıdır. Ödeme yapılan kişinin, önceki sahiplerinin daha önce işlem imzalamadıklarını doğrulayabileceği bir yönteme ihtiyacımız duyuyoruz. Hedeflerimiz için, ilk işlem en önemli işlemdir daha sonraki harcama girişimlerini umursamıyoruz. Bir işlemin gerçekleşmediğini onaylamanın tek yolu tüm işlemlerin farkında olmaktır. Merkezi otoriteye dayalı modelde, otorite tüm işlemleri bildiği için hangi işlemin önce geldiğine karar vermektedir. Bunu, güvenilen bir taraf olmadan başarabilmek için işlemlerin herkese duyurulması ve katılımcıların işlemlerin gerçekleştiği tarih sırası konusunda anlaşacağı bir sisteme ihtiyaç duyulmaktadır. Ödeme yapılan kişinin, yapılan her işlem sırasında harcamanın ilk kez yapıldığı taraf olduğunun diğer tarafların çoğu tarafından onaylandığı bir kanıta ihtiyaç duyar. [17]



Şekil 28: Eşler arası elektronik nakit ödeme sistemi
Kaynak: Bitcoin: A Peer-to-Peer Electronic Cash System

Sahip 1, sahip 2 ye Bitcoin göndermek istediğinde, Sahip 1 özel anahtarını kullanarak bir imza oluşturur. Daha sonra açık cüzdan adresinden sahip 2 nin açık cüzdan adresine bir transfer talimatı vererek bu imzayı ekler. Yapılan bu işlemin, sahip 1 tarafından oluşturulduğu tüm taraflar ile paylaşılmakta olan açık anahtar ile doğrulanabilir. Ancak, sahip 1 in elinde yeteri kadar Bitcoin olup olmadığı ve elindeki Bitcoini birden çok defa gönderip gönderemeyeceği konuları en önemli iki sorun olarak görülmektedir.

Karşımızda sorun olarak duran bu iki durumun çözümü için Blokzincir devreye girmektedir. Bitcoin üzerindeki tüm işlemler ağda bulunan herkesin görebileceği ama değiştiremeyeceği bir Blokzincir yapısı üzerinde bulunduğundan sahip 1 in hesabında ne kadar Bitcoin olduğu sorusu cevabını bulacaktır. Yeterli Bitcoini olmayan kullanıcıya transfer yapma izni verilmeyecektir. Yine aynı sistemle, sistem üzerinde

oluşturulan mutabakata dâhil olan tüm taraflarca sahip 1 in işlemleri kontrol edilerek kural dışılık tespit edilmesi halinde transfere izin verilmez.

Tezimizin mutabakat başlıklı kısmında bahsedildiği üzere Blokzincir teknolojisinde merkezi bir yapı olmayıp yapılan işlemlerin onaylanması için önceden belirlenmiş mutabakat vardır ve taraflar bu mutabakata uygun hareket etmek zorundandır.

Bitcoin sisteminde yeni BTC üretilebilmesinin tek yolu Blokzincir ağı üzerinde yeni bir bloğun oluşturulmasıdır. Her yeni blok, ağ içindeki mutabakat surecine katılan kullanıcılardan birisi tarafından oluşturulur. Blokzincir ağında yeni bir blok üretebilmek için ağ üzerinde yer alan mutabakat noktalarının sayısı ve işlem gücü ile doğru orantılı olarak matematiksel zorluk seviyesi farklılık gösteren bir problemin çözüm kümesinin bulunması gerekmektedir. Her yeni blok üretimi sonrasında ilgili bloğu üreten kullanıcıya emeğinin karşılığı olarak belli miktarda Bitcoin verilir.

Nakamoto, tasarladığı bu sistemde zamanla kullanıcı sayısının artacağını ve Bitcoin üretimine yüksek ilginin olacağını öngörmüş olacak ki Bitcoin üretimi için bazı kurallar belirlemiştir.

Sistem faaliyete geçtiği ilk zamanlarda, oluşturulan her blok için 50 Bitcoin üretilmekte idi. Sonrasında 210.000 blok üretildiğinde oluşturulan her blok için 25 Bitcoin üretilmeye başlanmıştır. Bir bloğun oluşturulması ortalama 10 dakika sürdüğünden 210000 blok yaklaşık dört yılda oluşturulmakta ve Ocak 2009 da faaliyete geçtiğinde 50 bitcoin üretilen sistemde Kasım 2012 de yarılanma (halving) olmuş ve 25 Bitcoin üretimine geçilmiştir. Temmuz 2016’ da gerçekleşen ikinci yarılanmadan sonra oluşturulan her bir blok için 12,5 Bitcoin üretilmeye başlanmıştır. Bu şekilde yarılanma devam ettiği takdirde 2140 yılında yaklaşık 21.000.000 Bitcoin üretildikten sonra yeni blok oluşturma işlemi yapılmayacaktır.

5.2. Ethereum

Bitcoin platformunun kripto para oluşturma ve eşler arası kripto para transferi için tasarlanmış olması, farklı alanlarda kullanımını sınırlandırmaktadır. Bu sınırlandırmanın önüne geçebilmek için Bitcoin platformunda alternatif yeni protokoller hazırlanmaya çalışılsa da bu alternatiflerin genelden ziyade özele hitap etmesi ve yüksek maliyeti sebebiyle farklı alanlara yönelik problemlerin çözümü için Ethereum platformu geliştirilmiştir.

Ethereum'un kurucularından Vitalik Buterin "Eğer kripto paralar ile dünyada bulunan değerli kaynakları karşılaştırırsak Bitcoin altın, Litecoin gümüş, Ethereum petroldür. Çünkü Ethereum'un altında yatan teknoloji dünyanın internet sistemindeki enerji kaynağı olacaktır. Dünyada petrol nasıl birçok sektör ve teknolojide kullanılıyorsa Ethereum teknolojisi için de aynı şey geçerlidir. Bu nedenle biz Ether'i 'kripto yakıt' olarak adlandırıyoruz. Ethereum platformunun ihtiyaç duyduğu enerji Ether (ETH) ile sağlanacak" şeklindeki açıklaması ile Bitcoin ve diğer altcoinler ile Ethereum'un farkını ortaya koymuştur. [6]

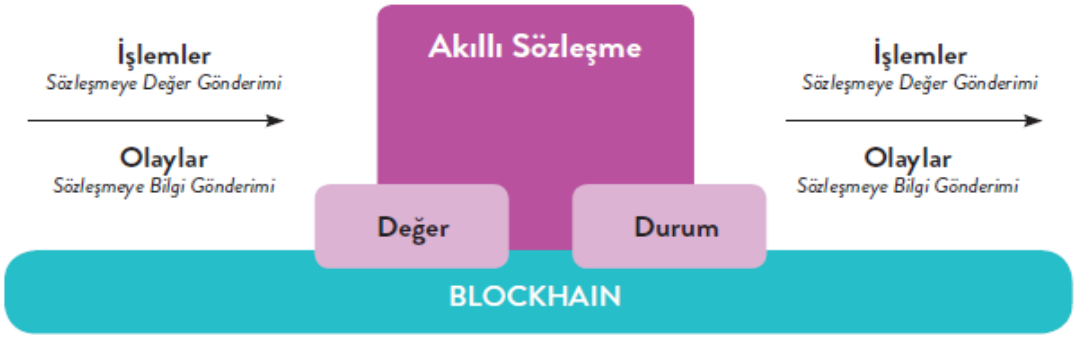
Ethereum ağ yapısında her makine Ethereum Virtual Machine (EVM) adı verilen bir sanal makine çalıştırır. Bu sanal makine, Ethereum tarafından sağlanan özel üst seviye programlama dilleri (Solidity, Viper, Serpent gibi) ile yazılmış herhangi bir uygulamanın Ethereum yapısı üzerinde çalışmasına izin vermektedir. Ethereum tarafından sağlanan dil yapıları "Turing-complete" olarak adlandırılan bir özelliğe sahip olduklarından, teorik olarak gözlemlediğimiz her şey Ethereum içerisinde bir program olarak hazırlanabilmektedir (bu programlara "Akıllı Sözleşmeler" adı verilir). Bu programlama yaklaşımı, çeşitli uygulamaların yazılmasına olanak sağlıyor olsa da şu andaki yapısı ile özellikle eşler arasında doğrudan etkileşimi otomatikleştirmeyi veya bir ağ üzerinden koordine edilen grup tabanlı aksiyonları kolaylaştırmayı hedefleyen uygulamalar için uygundur. [1]

Ethereum platformunun, Ether (ETH) adında bir kripto para birimi mevcuttur. Bu para birimi, Ethereum platformunda bulunan uygulamaların çalışmasında kullanılmakta olup platformun çalışmasında yaşanacak olumsuzlukları da bertaraf etmek için tasarlanmıştır. Bitcoin' de ortalama blok oluşturma süresi 10 dakika iken Ethereum bu süreyi 12-14 saniye olarak planlamaktadır.

5.2.1. Akıllı Sözleşmeler

Blokzincir ağları üzerinde çalışma alanı olan "Akıllı Sözleşmeler", bulunduğu ağ üzerinde oluşturulan bloklarda yer alan verilerin, önceden belirlenmiş durumları sağlaması halinde otomatik olarak çalışarak yine önceden belirlenmiş görevleri ifa etmesini sağlamaktadır. Örneğin; araba alım satım işlemi yapmak için notere ihtiyaç duyan taraflar, para transferini noter aracılığıyla yapamamaktadır. Bu durum mağduriyetlere yol açmaktadır. Oysaki araba devri ve satış bedeli transfer etme görevi olan bir akıllı sözleşme ile satış işlemi kolay ve güvenli biçimde gerçekleşir. Söz konusu akıllı sözleşmenin yer aldığı Blokzincir ağına arabayı satacak ve alacak tarafların kimlik bilgileri, arabanın kim tarafından satılıp kim tarafından alınacağı ve satış bedeli bildirildikten sonra akıllı sözleşme çalışmaya başlar ve ilgili kurumların veri tabanlarından satıcının arabaya ilişkin sahiplik bilgileri ile alıcının arabayı alacak yeterlilikte parası olup olmadığını kontrol eder. Kontrol sonrasında herhangi bir sorun yok ise, tarafların onayı ile birlikte otomatik olarak para transferi gerçekleşir ve arabanın sahiplik durumunda gerekli değişiklik yapılır.

Akıllı sözleşmeler bir bilgisayar ve matematik bilimcisi olan Nick Szabo tarafından 1994 yılında ortaya atılmıştır. 2013 yılının ikinci yarısında Vitalik Buterin tarafından Ethereum platformunu anlatan bir çalışma yayınlanmıştır. Bu çalışmada Akıllı Sözleşme kavramının kullanılması, söz konusu kavramın Blokzincir teknolojisi içinde kullanılmaya başlanmasına sebep olmuştur.



Şekil 29:Akıllı sözleşme
Kaynak: Blockchain 101

Akıllı Sözleşmeler, ilişkili tarafların anlaşmasından sonra hazırlanır, kriptografik olarak imzalanır ve Blokzincir ağına yüklenir. Yüklenen sözleşmeler ağ üzerindeki her bileşenle etkileşim kurabilir. Bu etkileşim işlem başlatmak, bilgi göndermek ve almak biçiminde olabilir. Sözleşmede taraflarca belirlenmiş olan durumlar akıllı sözleşme ile anlaşma koşullarına uygun olarak çalıştırılır. [1]

Her ne kadar akıllı sözleşmeler Ethereum Blokzincir ağı ile özdeşleşmiş olsa da Blokzincir platformlarının önemli bir kısmı akıllı sözleşme yapılasına destek vermektedir.

Akıllı sözleşmeler, merkezi otoriteye ve aracı kurumlara ihtiyacı azaltmakla birlikte yazılım tabanlı olduğundan insandan kaynaklanan hataları ortadan kaldırıp, işlem süresinin kısalmasını sağlar. Ayrıca insan kaynağı ihtiyacını azalttığından maliyetleri düşürür.

Hâlihazırda var olan Blokzincir ağlarında işlemlerin kontrol edilip yeni bir blok oluşturulması oldukça fazla zaman almaktadır. Günümüzde kullanımı yaygın olan ve Blokzincir temelli olmayan veri tabanlarında saniyede binlerce işlem yapılabilirken Blokzincir platformlarında saniyede en çok 20 işlem yapılabilmektedir.

Blokzincir yapıları kriptografik olarak veri güvenliği sağlıyor olsalar da Blokzincir ağları üzerinde yapılan akıllı sözleşme tanımlarında, kullanılan platformların yapısının doğru anlaşılmaması kaynaklı hatalı uygulamaların ortaya

çıktığı gözlemlenmiştir. Singapur Ulusal Üniversitesi tarafından yapılan akademik bir çalışmada Ethereum üzerinde tanımlı 19.366 akıllı sözleşmeden 8.833 tanesinde, sözleşmenin manipüle edilip sonucunda kazanç elde edilebilecek güvenlik açıklarının olduğu tespit edilmiştir. [1]

5.3. Hyperledger

2015 yılının Aralık ayında Linux Vakfı tarafından başlatılan Hyperledger, açık kaynak kodlu bir Blokzincir platformudur. Platform tek bir Blokzincir yapısından öte içerisinde farklı alt projelere destek verebilecek şekilde tasarlanmıştır.

Hyperledger bir kripto para değildir. Linux Vakfı'nın bu platformu oluşturmaktaki amacını; iş dünyasına hem ticari hem de teknik yönetimler tarafından destek verilen tarafsız ve açık altyapılar sağlamak, insanları Blokzincir konusunda eğitmek ve gelişime açık teknik topluluklar kurmak olarak açıklayabiliriz. Platformun üyeleri arasında American Express, Cisco, J.P.Morgan, Intel, IBM, SAP, Digicert, FedEx, Huawei, Oracle gibi şirketler bulunmaktadır.

Hyperledger, servis katmanı ve bu servislerin dünya üzerinde kullanılmasına olanak sağlayan Hyperledger API(Application Programming Interface – Uygulama Programlama Arayüzü)/SDK(Software Development Kit – Yazılım Geliştirme Kiti) katmanı olmak üzere iki kısımdan oluşur.

Hyperledger servis katmanı; üyelik servisleri, Blokzincir servisleri ve Ethereum Platformundan aşina olduğumuz Akıllı Sözleşmelerin Hyperledger Platformundaki karşılığı olan chaincode servisleri adı verilen üç ana mantıksal katmandan oluşmaktadır. Kimlik, şifre vb. kullanıcı işlemleri için üyelik servisleri, mutabakat yönetimi için Blokzincir servisleri kullanılırken mutabakatların işletimi için ise chaincode servisleri kullanılmaktadır.

Verilerin herkese açık bir ağ üzerinde tutulması ve isteyen herkesin veriye ulaşabilmesinden kaynaklı sorunların önüne Hyperledger ile geçilebilir. Hyperledger kullanılarak belirli bir kullanıcı grubuna ait bilgiler saklanabilmektedir. Ayrıca,

kullandığı modüler mimari sayesinde geliştiriciler hali hazırda kullandıkları bir modülü Hyperledger projesine ekleyebilirler.

Hyperledger projelerinden en bilineni Hyperledger Fabric Projesidir. Hyperledger Fabric bir Blokzincir çerçeve uygulaması ve Linux Vakfı tarafından barındırılan Hyperledger projelerinden biridir. Modüler bir yapıya sahip uygulamalar veya çözümler geliştirmek için bir temel olarak tasarlanan Hyperledger Fabric, fikir birliği ve üyelik hizmetleri gibi bileşenlerin tak-çalıştır özellikli olmasını sağlar. Hyperledger Fabric, sistemin uygulama mantığını oluşturan chaincode adı verilen akıllı sözleşmelere ev sahipliği yapmaktadır.

5.4.Ripple

Ripple platformunun kurucularından Ryan Fugger 2004 yılında merkezi olmayan, güvenli ve online bir para sistemi kurmak ve kişilerin kendi para birimlerini oluşturmalarını sağlamak amacıyla Ripplepay projesini geliştirdi. Bu proje, birbirini tanıyan insanlar arasında karşılıklı olarak borçların ödenmesi amacıyla kullanılmıştır.

Bu projeden esinlenen Jed McCaleb, Arthur Britto, David Schwartz ile birlikte Ryan Fugger; işlemlerin Bitcoin platformundaki gibi madencilik faaliyetinden ziyade kullanıcılar arasındaki gerçekleşen oy birliği süreciyle doğrulandığı dijital para birimi sistemini 2011'de geliştirmişlerdir. Ripple adı verilen sistemde madencilik faaliyeti olmadığından daha az elektrik enerjisi harcanmaktadır. Bitcoin platformunda, sistemde yer alan tüm katılımcıların senkronize olarak iletişim halinde olması gerektiğinden süreçler yavaş ilerlemekte iken Ripple sistemi ise sistem içinde güvenilir alt ağlar oluşturan bir algoritma tarafından geliştirilmiştir. [18]

Ripple büyük tutarlı ödemelerin gerçek zamanlı olarak yapıldığı bir mutabakat sistemi, yabancı para birimi takası platformu ve merkezi olmayan bir havale ağıdır. Ripple mevcut ödeme ağlarına uluslararası gerçek zamanlı ödeme olanakları ile birbirleri arasında irtibat kurma olanağı sağlayan teknolojik bir altyapı olarak da hizmet vermektedir. SWIFT ve Western Union gibi uluslararası para gönderme sistemlerinde var olan yüksek maliyet ve yavaşlık sorunları ile muhatap olmamak üzere geliştirilmiştir.

Ripple platformu, diğer Blokzincir platformlarında kullanılan PoW ya da PoS mutabakat yöntemleri yerine kendisine özel interledger protokol isimli bir mutabakat yapısı kullanmaktadır. Bu protokol, tasarımı itibari ile küresel bir koordinasyon sistemine ya da Blokzincir yapısına ihtiyaç duymamaktadır. Bu protokol sayesinde Ripple işlemlerini saniyeler içerisinde tamamlayabilmektedir.

Platform, XRP adında kripto para birimine sahip olsa da yapısı gereği para birimlerinden bağımsız bir sisteme sahiptir. Ripple üzerinde, kripto para birimleri de dahil olmak üzere her para birimi ve hatta değer ifade eden mil puan gibi herhangi bir birim ile de işlem yapılabilmektedir.

Ripple firması tarafından geliştirilen ve kripto para borsalarında işlem gören XRP, doğrudan Ripple servisine bağlı değildir. Bu nedenle Ripple firmasının başarısı ile XRP'nin borsadaki değeri arasında doğrudan ilişki bulunmamaktadır.

Ripple platformunda yer alan kullanıcılar (Ripple entegrasyonu olan finansal kurumlar), güvendikleri kullanıcıları ve bu güven yapısı içerisindeki işlem bilgilerini (limit vb.) tanımlamak zorundadırlar. Ripple platformu, iki kullanıcı arasında yapılan bir para transfer işleminde öncelikli olarak bu iki kullanıcı arasında güvenli bir iletişim kanalı kurmaya çalışır. Direk bir iletişim kanalı oluşturamaması durumunda, kullanıcıların güvendikleri diğer yapıları kullanarak bu iletişimi oluşturmaya çalışır (gerekirse bunun için kendi kripto para birimi üzerinden dönüşüm gerçekleştirir). Bu güvenli yol kurulduktan sonra tüm işlemler atomik yani işlem bütünlüğünün bozulmadığı (işlemlerin ya hepsi gerçekleşir ya da hiç biri gerçekleşmez, parçalı bir gerçekleşme durumu oluşmaz) bir şekilde gerçekleşmektedir. [1]

Ripple platformu uluslararası alanda birtakım finans kurumları tarafından denenmektedir. Alman Reisebank ve Kanadalı ATB bank arasında yapılan Ripple testlerinde, hali hazırda dört gün kadar süren para transferinin 8 saniye içerisinde gerçekleştiği gözlemlenmiştir. Ülkemizde bankalarından Akbank, Ripple ağına dâhil olan bankalar arasındadır. 2018 yılında Akbank ile Santander UK bank arasında Ripple üzerinden İngiliz sterlini transferi başlamıştır.

6. DÜNYADA BLOKZİNCİR

Türkiye'nin ilk üniversite Blokzincir merkezi İstanbul Blockchain ve İnovasyon Merkezi (BlockchainIST Center**),** Bahçeşehir Üniversitesi'nde 2018 yılında hizmete açıldı.

Merkez, Blokzincir teknolojileri alanında bilimsel çalışmalar ve yayınlar yapmayı, piyasadaki Blokzincir uzmanı açığını kapatmayı, araştırma geliştirme ve inovasyon merkezi olmayı hedeflemektedir. Üniversite; diploma, sertifika ve transkript gibi belgelere zaman kaybetmeden ulaşmayı sağlayacak sistemi geçtiğimiz< aylarda hayata geçirdi. İlk olarak BAU International University Washington D.C kampüsünde hayata geçen CertifyIST, diğer kampüslerdeki öğrencilerin de sertifika, diploma ve öğrenimlerine dair her türlü belgenin tutulabileceği bir uygulamadır. CertifyIST, hem mobil hem de web sitesi uygulamasıdır.

Uygulama ile öğrencilerin kaybolan belgelerinin yeniden istenmesi durumunda oluşan vakit kaybı ortadan kaldırılıp sahte diploma olayının da bitirilmesi hedeflenmektedir. CertifyIST uygulamasının içerisindeki akıllı sözleşmeler ile diplomaların sahtesinin üretilmesi mümkün olmayacak, sadece izin verilen kurumun o diplomayı çıkardığı ispatlanmış olacaktır.

Malta, 2018 yılında Blokzincir teknolojisi ile alakalı üçlü bir yasa çıkarmış ve aşağıdaki kurumları kurmuştur.

- Malta Dijital Yenilik Kurumu (MDIA): Kurum, dijital yenilik otoritesi olarak dağıtık defter teknoloji platformlarının denetlenmesi ve akıllı sözleşmelerin onaylanması görevlerini üstlenmektedir.
- Yenilikçi Teknoloji Anlaşmaları ve Hizmetleri Kurumu (ITAS)
- Dijital Finansal Varlıklar Kurumu (VFA): Dijital paranın piyasaya sürülmesi konusunda çerçeve ve yükümlülükleri belirler. [19]

Estonya Hükümeti 2016 yılında 1.3 milyon vatandaşının sağlık kayıtlarını güvence altına almak için Blokzincir teknolojisine yöneldi. Tamamen dijital bir toplum oluşturma hedefinde olan ülkede Estonya E-Sağlık Vakfı 2016 yılında vatandaşlarının doktor, hastane, hastalık, tetkik vb. sağlık kayıtlarının arşivlenmesinde Bokzinciri teknolojisini kullanarak hasta sağlığı kayıtlarını koruma amaçlı Blokzinciri projesini başlattı. [20]

İngiltere' de 2017 yılında kurulan İngiliz Blokzincir Derneği (The British Blockchain Association) İngiltere'de halka açık ve özel sektörlerde Blokzincir teknolojisinin benimsenmesini destekleyen, kar amacı gütmeyen, üyelik destekli bir organizasyondur. Avrupa'nın Blokzincir ekosistemi üzerine hakemli ilk araştırma dergisi olan Journal of British Blockchain Association'a ev sahipliği yapmaktadır. [21]

Birleşik Arap Emirlikleri, Blokzincir teknolojisi çalışmalarına yeterli kaynağı ayırmakta ve çalışmalar oldukça hızlı ilerlemektedir. Dubai hükümeti şu anda 20 proje üzerinde çalışmaktadır. Hükümet, Dubai'yi "dünyanın en akıllı ve en mutlu şehrine" dönüştürmek amacıyla şehir çapında bir girişim olan Smart Dubai'yi hayata geçirmek için IBM ile ortaklık kurmuştur. Dünyanın ilk Blokzincir destekli hükümeti olmayı hedefleyen Dubai Hükümeti 2018 nisanında hükümet işlemlerinin % 50'sinde Blokzinciri teknolojisinden faydalanmak amacıyla Emirates Blokzincir Stratejisi 2021(Emirates Blockchain Strategy 2021) adlı projeyi başlatmıştır. [22]

İsveç Hükümeti toprak mülkiyeti, ulusal haritalama, kadastro ve toprak kayıt otoritesi Lantmäteriet, mülk işlemlerinin Blokzincir teknolojisi kullanılarak yapılması için 2016 yılında çalışmaya başladı. Lantmäteriet, telekomünikasyon şirketi Telia, danışmanlık şirketi Kairos Future ve Blokzincir teknoloji şirketi ChromaWay ile ortaklık kurdu ve emlak anlaşmaları yapmak için blok zinciri tabanlı bir platform geliştirdi. İkinci denemeyi 2017 yılında yapan Lantmäteriet, Temmuz 2018 de söz konusu projenin pilot uygulamasını gerçekleştirdi. [23]

Küresel araba üreticileri, araçlarında kullandıkları maddelerin etik bir kaynaktan olduğunu kanıtlama konusunda baskı altındalar. İnsanlar, araçlarda kullanılan maddeler için çocuk işçilerin çalıştırılıp çalıştırılmadığını ya da bir silahlı çeteyi finanse etmek için kullanılmadığını bilmek istemektedir. Volvo, kullanılan

materyallerin etik kaynaklı olduğunu kanıtlamak amacıyla tedarik zincirini izleyebilmek için Blokzincir tabanlı bir çözümü test etti ve bu testlerin sonucunda Blokzincir teknolojisiyle takip edilen ve geri dönüşümlü kobalt maddesi kullanılan ilk araçları başarıyla ürettiklerini duyurdu. Şirket, kullandıkları dağıtık defter teknolojisinin tedarik zincirlerinde hesap verilebilirliği ve şeffaflığı artırdığını tespit etmiştir. Bunun için Oracle ile iş birliğine giden şirket aynı zamanda İngiltere merkezli Blokzincir girişimi Circulor ile de birlikte çalışmakta olup tedarik zinciri izleme sisteminin bu yılın sonuna kadar şirket geneline yayılması beklenmektedir. [24]

İsviçre merkezli gıda devi Nestlé, ürünlerini tedarik zinciri boyunca takip etmek için Blokzincir teknolojisini kullanacağını açıkladı. WWF-Avustralya ve BCG Digital Ventures tarafından kurulan Blokzincir platformu OpenSC ile birlikte geliştirilecek olan proje, Nestlé'nin ürünlerini tedarik zinciri boyunca şeffaf bir şekilde izlemesini sağlayacaktır. Nestlé'nin iddiasına göre kendileri, açık Blokzincir teknolojisini bu şekilde kullanan ve pilot programını başlatan ilk büyük yiyecek ve içecek şirketi oldu. Şirket OpenSC platformuyla birlikte tüketicilerin bağımsız olarak doğrulanabilir tedarik zinciri verilerine ulaşabileceğini belirtmektedir. Pilot uygulama ilk olarak Yeni Zelanda'daki çiftliklerden ve üreticilerden Orta Doğu'daki fabrikalara ve depolara giden sütleri izleme imkânı sunacaktır. Ayrıca şirketin Amerika Kıtası'nda üretilen Palm yağına bu takip sürecini getirmesi bekleniyor. [25]

Güney Avustralya Hükümeti, Blokzincir çözümleri sağlayan Horizon State şirketiyle seçimlerde Blokzincir teknolojisinden faydalanmak üzere bir anlaşma imzaladı. Yeni Zelanda merkezli şirketin yaptığı açıklamaya göre Horizon State, oylama esnasında hükümete destek olmak amacıyla Blokzincir teknolojisini kullanacak.

Küresel teknoloji devi Sony ve BT firması Fujitsu gerçekleştirdikleri iş birliği ile dil sertifikalarının doğruluğunu Blokzincir altyapısı ile kontrol edecekler. Buna göre, Sony ve Fujitsu arasında gerçekleşen iş birliği ile özel bir veri tabanı sistemi geliştirildi. Bu sistem Blokzincir teknolojisini kullanmakta olup eğitim sertifikalarının sahte olup olmadığını kontrol etme amacını taşımaktadır. Sistem Japonya'daki eğitim veri tabanlarına erişerek iş başvurusu ve çeşitli süreçlerde yabancılar tarafından sunulan dil bilgisi sertifikalarının doğruluğunu kontrol etmektedir. Japonya'da

çalışmak isteyenler zaman zaman dil sertifikalarının yasadışı kopyalarını oluşturabilmektedir. Sony ve Fujitsu, Mart 2018' de platformu Osaka, Saga ve Tokyo şehirlerinde Japonca okulları yöneten Human Academy Co. ile birlikte test ettikten sonra Nisan 2018' de saha uygulamalarına başlamıştır. [26]

Bankalararası Kart Merkezi, Microsoft ve VeriPark ortaklığı ile geliştirilen belgem.io projesi ile eğitim sertifikaları Blokzincir tabanlı olarak dijital ortamda saklanmakta olup proje sayesinde kullanıcılar, aldıkları eğitim sertifikalarını güvenli bir şekilde Blokzincir altyapısı ile saklayıp diledikleri kurum veya kişilerle paylaşabilmektedir. Dijital bir belge platformu olan belgem.io, eğitim sertifikalarının özel bir Ethereum Blokzincir platformunda saklanması, görüntülenmesi ve paylaşılmasını sağlamaktadır.

Singapur merkezli Blokzincir girişimi Perlin, Uluslararası Ticaret Odası (ICC) ile yaptığı iş birliği kapsamında ICC' nin 130'dan fazla ülkede temsil ettiği 45 milyon üye işletmeyi Blokzincir ile tanıştırmayı planlamaktadır. Hali hazırda Asya-Pasifik Bölgesi'ndeki birçok büyük şirket için Blokzincir projeleri yürüten Perlin, artık yenilikçi teknolojilerini ön plana çıkarmak için ICC' nin üyelerine de erişim imkânı vermektedir. 1919 yılında kurulan ICC altında 45 milyon üye işletme barındırıyor. Bu işletmeler arasında Amazon, CocaCola, FedEx, McDonalds ve PayPal gibi birçok dev şirket de bulunmaktadır. Bahsi geçen ortaklık çeşitli biçimlerde olacak ancak daha çok üretim ve teslimat aşamalarında malların takip edilebilmesi için değer zinciri izlenebilirliğine odaklanılacaktır. [27]

Tayland'ın en büyük ticari bankası Siam Commercial Bank (SCB) ve devlete ait petrol şirketi PTT Exploration and Production Public Company Limited (PTTEP) arasındaki Blokzincir pilot testi başarıyla sonuçlandı. Operasyonel verimliliği iyileştirmek için yapılan çalışmalarda, geleneksel yöntemlerle iki güne kadar süre alan ödeme işleminin, Blokzincir üzerinden yapıldığında bir dakikadan daha kısa sürede tamamlandığı tespit edildi. Yıllık geliri 2,9 milyar doların üzerinde olan SCB, Tayland'ın en büyük ticari bankası olarak biliniyor. [27]

ABD ‘de Batı Virginia ve Denver’da yapılan seçimlerin ardından Blokzincir tabanlı mobil uygulama aracılığıyla oylama sistemini kullanan üçüncü bölge Utah eyaletinin ilçelerinden biri olan Utah County oldu. Utah County mobil seçim platformu Voatz, Tusk Philanthropies ve Ulusal Siber Güvenlik Merkezi ile iş birliği içinde gerçekleştirildi. 28 Haziran’da başlayıp 13 Ağustos’a kadar devam eden platformun pilot seçmenleri arasında aktif görevdeki ordu mensubu kişiler ve yurt dışındaki seçmenler yer almıştır.

Çin, Blokzincir teknolojisini finansal hizmetler, kamu hizmetleri, sağlık hizmetleri, tedarik zincirleri, akıllı üretim ve lojistik gibi çeşitli sektörlerde yaygın olarak kullanmaktadır. 2018 Kasım ayı itibariyle dünya genelindeki Blokzincir projelerinin %25 i Çin’ de yürütülmektedir. Çin'deki 615 Blokzincir platformu geliştiricisinden biri olan Qulian Technology, Zhejiang eyaletinin başkenti Hangzhou'da şirketler, devlet kurumları ve sanayi ittifakları için işletme düzeyinde ağ çözümlerine odaklanan Hyperchain'ı başlattı. Haziran ayında şirket, o sırada iç blok zinciri sektöründeki en büyük miktar olan 1.5 milyar yuan (222 milyon $) değerinde bir dizi B finansman turu elde ettiğini açıkladı. Qulian Technology' nin baş teknoloji sorumlusu Li Qilei Blokzincirin yeşil enerji ve akıllı devlet gibi diğer alanlarda da uygulanabileceğini söyledi. Qulian ayrıca sahte konut bilgilerinin çevrimiçi görünmesini engellemek amacıyla güvenilir bir emlak zinciri oluşturmak için bazı konut bürolarıyla birlikte çalışıyor. İnternet devleri Baidu, Alibaba ve Tencent toplu olarak kendi Blokzinciri girişimlerini başlattılar. [28]

Alibaba, 2016'dan bu yana kamu yararı, gıda ve sağlık gibi alanlarda Blokzinciri teknolojisini kullanıyor. Şirket, 90 blok zinciri patenti ile Blokzincir Kurumsal Patent Sıralamasında 1 numara oldu. 2018 Ağustos ayında, Guangdong eyaleti, Shenzhen’deki vergi bürosu ve Tencent, Çin’in ilk blokzinciri elektronik faturasının düzenlendiğini açıkladı.

Eskiden Baidu Finance olarak bilinen Du Xiaoman Financial, tüketici finansmanı, finansal müşterilerin yönetimi ve topluluk inşası yönetimi, varlıkların dijitalleştirilmesi, kamu refahı, kimlik sistemleri, dijital içerik telif hakkı, farklı ürünler arasındaki ara bağlantı ve takip olmak üzere sekiz alanda uygulama geliştirme kabiliyetini ana hatlarıyla açıklayan Blokzinciri beyaz kâğıdını yayımladı.

Uganda hükümeti, ülkedeki sahte ilaçları izlemek için BlockCon'un başlattığı MediConnect ile ortaklık kurdu. Uganda Başkanı Yoweri Musevini, Sağlık Bakanı Jane Ruth Aceng ve diğer hükümet yetkilileri, MediConnect'in ilaç sektöründeki çeşitli meseleleri ele almak üzere tasarlanan Blokzincir tabanlı platformuna destek verdi. Hükümet, sahte ilaçları takip etmek için platformu kullanacağını belirtti. Platform ile reçeteli ilaçların kaydedilmesi, sahte ilaçların tanımlanması ve farmasötik (Eczacılık biliminin temel yapı taşı olan "farmasötik kimya", ilaç hazırlarken kullanılan maddelerin, bileşenlerin, test ve deneylere dayalı olarak içerik oluşturulması işleminde yararlanılan bir bilim dalıdır.) tedarik zincirinde dağılımlarının engellenmesi hedeflenmektedir. [29]

2017 yılının başından bu yana, AB üye ülkeleri ile işbirliği içinde Avrupa Gümrük Birliği için politikaların oluşturulmasından sorumlu olan Vergilendirme ve Gümrük Birliği Genel Müdürlüğü (DG TAXUD), gümrük ve vergi alanlarında Blokzincir teknolojisi üzerine çalışmalar yürütmekte olup kurumun ilgi alanlarından birisi ATA Karnesidir. Uluslararası Ticaret Odası (ICC) ve Dünya Odaları Federasyonu (WCF), ATA Karnesini dijitalleştirmek için bir pilot projeyi 20 Haziran 2018 tarihinde başlattı. ATA Karnesi Mercury II olarak bilinen proje ile ATA Karnesindeki süreçleri dijitalleştirilip, işlemlerin hem işletmeler hem de gümrük idareleri için daha kolay ve daha verimli hale getirilmesi hedeflenmektedir. [30]

Singapur Para Otoritesi (MAS) ve Hong Kong Para Otoritesi (HKMA), 15 Kasım 2017 tarihinde Hyperledger Fabric ' i temel alan Global Trade Connectivity Network (GTCN) projesini duyurdu. Proje ile ticaret ve ticaret finansmanının dijital hale getirilmesi hedeflenmektedir. GTCN; sözleşmelerin, faturaların ve konşimentoların kâğıt bazlı geleneksel ticaret finansmanı işlemlerini ortadan kaldırmak amacıyla tasarlanmıştır. [31]

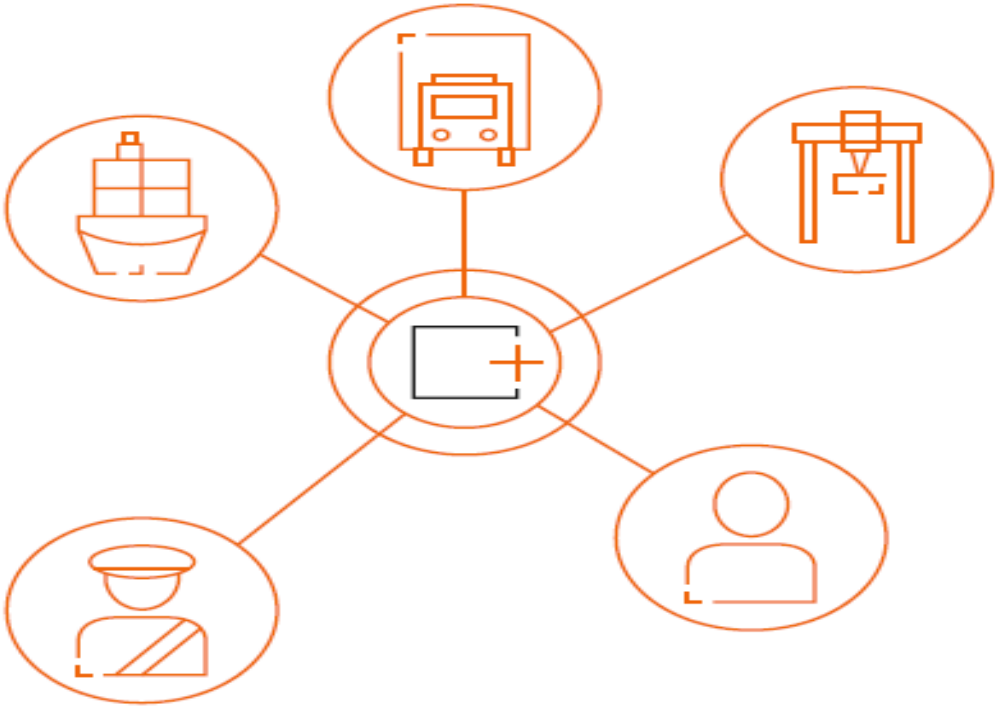
6.1. TradeLens

TradeLens, Blokzincir teknolojisi ile desteklenen açık ve nötr bir tedarik zinciri platformudur. Platform, endüstri çevresinde yenilikleri teşvik etmek, bilgi paylaşımını ve şeffaflığı desteklemek üzere çeşitli tarafları bir araya getiren daha etkili ve güvenli küresel işleri desteklemek üzere tasarlanmıştır. TradeLens verileri doğrudan kaynaktan yayınlanmaktadır. Bu sayede insanlar tedariklerini güvenli bir şekilde yönetebilmektedir. [32]

9 Ağustos 2018 tarihinde oluşumu duyurulan TradeLens ile dünyanın en büyük deniz taşımacılığı operatörlerinden olan Maersk, uluslararası sularda gemi taşımacılığıyla yapılan ticarette zaman ve maliyetten kazanmak, sürecin hızlanması ve evrakların prosedüründen kurtulmak amacıyla IBM ile stratejik iş birliği yoluna giderek Blokzincir altyapısını kullanmaya başlamıştır. TradeLens, Maersk ile IBM arasında yapılan işbirliği anlaşmasının bir sonucudur. Ülkemizden Güler Dinamik Gümrük Müşavirliği A.Ş. Ümit Bisiklet San. Ve Tic. A.Ş. ve PLH Lojistik Hizmetleri A.Ş. platformun katılımcıları arasında yer almaktadır. Platformda 154 milyondan fazla işlem kaydı bulunmakta ve günlük işlem kaydı bir milyon kapasiteye doğru yaklaşmaktadır.

TradeLens'in erken benimseme programının bir parçası olarak IBM ve Maersk ile birlikte 94 kuruluşun aktif olarak TradeLens platformunda yer aldığı bilinmektedir.

TradeLens, tedarik zincirindeki tüm tarafları bir araya getirir. Kargo sahipleri, nakliye firmaları, kara yolu ve demiryolu taşımacılığı firmaları, liman ve okyanus taşımacılığı işletmeleri, gümrük ve diğer devlet yetkililerini güvenli veri paylaşımı ve işbirliği için bir araya getirmek amacıyla kurulan bir platformdur. Platform, ithalat ve ihracat izni dâhil olmak üzere Blokzinciri sayesinde iş süreçlerinin otomasyonunu, temel işlem bilgilerinin güvenli, değişmez ve denetlenebilir olmasını sağlar. [32]



Şekil 30: TradeLens Ekosistemi

Kaynak: TradeLens Solutıon Brıef Edition two

TradeLens ekosisteminde;

Dünya çapında, Hong Kong'da PSA Singapore, International Container Terminal Services Inc, Patrick Terminals, Modern Terminals, Port of Halifax, Port of Rotterdam, Port of Bilbao, PortConnect, PortBase ve Port of Phladelphia'daki Hold Logistics Terminal operatörlerinin kılavuz çözümündeki ağı dâhil olmak üzere 20'den fazla liman ve terminal operatörü yer almaktadır. Bu da TradeLens' e aktif olarak katılan ya da katılacak olan yaklaşık olarak dünya çapındaki 234 deniz ağ geçidine denk gelmektedir. Bu çözüm platformuna katılan global konteyner taşımacılığı yapan firmalar arasında Hamburg Süd ile Pacific International Lines' da bulunmaktadır. Hollanda, Suudi Arabistan, Singapur, Avustralya ve Peru'daki gümrük idareleri de Ransa ve Güler Dinamik Gümrük Müşavirliği A.Ş. firmaları ile birlikte katılım sağlamaktadır. Agility, CEVA Logistics, DAMCO, Kotahi, PLH Lojistik Hizmetleri A.Ş. Ancotrans ve WorldWide Alliance'ı da kapsayan Nakliyeciler, taşımacılık ve lojistik firmaları şu anda katılımda bulunanlar arasında yer almaktadır. [33]

TradeLens Ekosisteminin faydaları kısaca;

“Sevkiyat hatlarında önceden oluşturulmuş bağlantılar sayesinde, eşyanın sevkiyatında baştan sona görünürlük ve gerçek bilgiye gerçek zamanlı erişim,

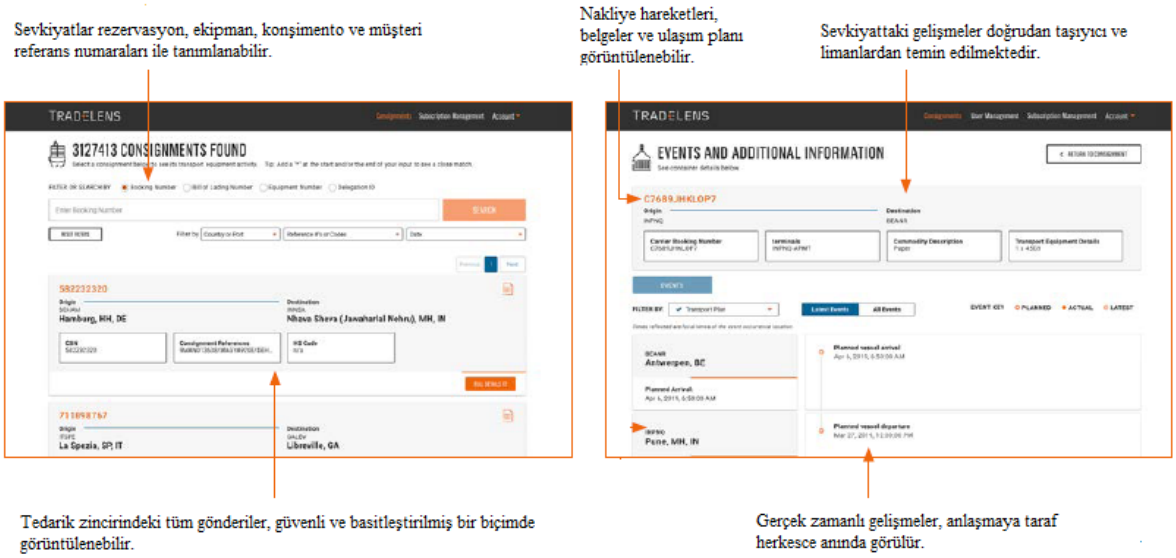
Eşyanın sevkiyatında uçtan uca dijital denetim nedeniyle azalan müşteri hizmetleri ve ağ uyum maliyeti, daha az gelir sızıntısı ve daha az yanlış beyan,

Hükümet yetkilileri açısından daha bilinçli risk değerlendirmeleri, daha iyi bilgi paylaşımı, daha az manuel evrak ve ulusal tek pencere platformlarına daha kolay bağlantılar,

Göndericiler ve alıcılar açısından daha fazla tahmin edilebilirlik, sorunların erken bildirimi, süreçlerde tam şeffaflık,

Ticaret finansmanı ve ticaret sigortası için kesin ve gerçek zamanlı bilgiye erişim.“ olarak ifade edilebilir.

TradeLens'i kullanan ithalatçılar ve ihracatçılar, Gönderi Yöneticisi Kullanıcı Ara yüzü aracılığıyla veya bir olay özet akışına abone olarak ve TradeLens verilerini mevcut sistemlerine entegre ederek gönderilerinin durumunu kolayca takip edebilirler. Platform, ticari taraflar arasında doküman paylaşımı için güvenlik, versiyon kontrolü ve mahremiyet ile çerçeve sağlar. Gerekli izinlere sahip yetkili kullanıcılar sisteme yükleme yapabilir, belge görüntüleyebilir, indirebilir ve belge üzerinde düzenleme yapabilir. TradeLens belge deposu, belgelerin taraflarca güvenli bir şekilde saklanmasını, görüntülenmesini ve işlem görmesini sağlar. [32]



Şekil 31:Gönderi Yöneticisi Kullanıcı Ara yüzü

Kaynak: TradeLens Solutıon Brıef Edition two

TradeLens Blokzinciri, işlemleri kayıt altına alan ve maddi veya maddi olmayan duran varlıkları izleyen ortak ve değişmez bir defterdir. TradeLens'in gücü ekosistem üyelerinden gelirken, Blokzincir teknolojisi platformun kalbi olan hayati bilgilerin güvenli bir şekilde dağıtılmasını ve depolanmasını sağlar.

Ağ katılımcıları, hiçbir zaman bir belgenin gönderilmesini beklemek zorunda kalmadan, paylaşılan belgelere ve verilere hemen erişebilir. Bir belge TradeLens platformuna yüklendiğinde veya var olan belge düzenlendiğinde belgenin yeni bir sürümü oluşturulur ve belge deposuna eklenir. Böylece birden fazla kopya ve en son sürümleri tanımlamanın tutarsızlığı ortadan kalkar.

TradeLens, üyelerinin kriptografik kimliklere dayanarak ağ tarafından bilindiği açık kaynaklı izinli bir blok zinciri olan Hyperledger Fabric'i temel alan IBM Blokzincir Platformunu kullanır. [32]

Sayısallaştırılmış belgeler ve izin verilen paylaşımla TradeLens, kâğıt kullanılan eski iş akışlarından uzaklaşarak, maliyetli, tekrarlayan ve hataya elverişli manuel girdilerden vazgeçen birden fazla kuruluştaki otomatik iş akışlarına geçişi kolaylaştırır.

Şekil 32:TradeLens Otomatik İş Akışı

Kaynak: TradeLens Solutıon Brıef Edition two

6.2. Networked Trade Platform (NTP)

Networked Trade Platform (NTP), Singapur'a dünyanın önde gelen ticaret, tedarik zinciri ve ticaret finansman merkezi olma temelini oluşturan ulusal bir ticaret bilgi yönetimi platformudur. NTP; işletmeleri, topluluk sistemlerini, platformları ve hükümet sistemlerini birbirine bağlayan bir ticaret ve lojistik ekosistemi oluşturmak için endüstri çapında bir dijital dönüşüm sağlamak için harcanan çabayı göstermektedir. [34]

Vizyonu, Singapur'un dünyanın önde gelen ticaret, tedarik zinciri ve ticaret finansman merkezi olması için temel oluşturan ulusal bir ticaret bilgi ekosistemi olmaktır. Hükümetin mevcut TradeXchange ve TradeNet platformlarının yerini alacak olan NTP, kâğıt üzerinde yapılanları dijitalleştirerek üretkenliği arttırmayı, daha doğru veri analizi yaparak rekabetçiliği artırmayı ve üçüncü taraf servis sağlayıcıları için fırsatlar yaratmayı amaçlamaktadır.

Yatırımcılar, lojistik hizmet sağlayıcıları, taşıyıcılar ve bankalar ticari süreçlerin dijitalleşmesi ve düzenlenmesine yardımcı olacak ticaret bilgi ekosistemi olarak hizmet verecek yeni bir tek elden ticaret platformu olan Networked Trade Platform (NTP) ile birbirine bağlanacaktır. 26 Eylül 2018'de Maliye Bakanı Bay Heng Swee Keat tarafından başlatılan platform, ticari değer zinciri boyunca oyuncuları tek bir platforma sokarak, uçtan uca dijital ticareti mümkün kılacaktır. [35]

NTP, ticaret işlemlerinde tamamen kâğıtsız olarak işlem yaparak, yatırımcıların zamandan ve maliyetten tasarruf etmesine ve doğru veriye ulaşmasına yardımcı olur.

NTP' de dört devlet hizmeti de mevcuttur ve bu hizmetler aşağıda verilmiştir.

Serbest satış belgesi: Belirtilen malların Singapur'da serbestçe satıldığını gösteren bir belge.

Manipülasyonsuzluk Belgesi: Singapur üzerinden gönderilen malların transit sırasında değiştirilmediğinin ispatı olan belgedir.

İthalat Sertifikası ve Teslimat Doğrulaması: İthalat Sertifikası ve Teslimat Doğrulaması, ihracatçı ülkelerin Singapur'a hassas ihracatlarının Singapur'daki belirli bir son kullanıcı için yapıldığına ve üçüncü bir ülkeye yönlendirilmediğine dair endişelerini gidermeye yardımcı olmaktadır.

İniş Sertifikası: Bir gümrük izin belgesinde beyan edilen malların inişine ve Singapur'a ithal edildiğine dair sertifikadır. Ayrıca yolculuk / uçuş detayları, yükleme limanı, gümrük izin numarası ve gümrük tarihini de içermektedir. [36]

Singapur Devleti, NTP' nin uluslararası ticaret bağlantılarını güçlendirmek için birçok girişimde bulunmaktadır. Bu kapsamda, Singapur'un Finans Daimi Sekreteri Tan Ching Yee ve Çin'in Singapur Büyükelçisi Hong Xiaoyong, 12 Kasım 2018 tarihinde uluslararası ticarette Tek Pencere işbirliği konusunda ticareti kolaylaştırmak için bir çerçeve anlaşma imzaladı. Teknolojiden yararlanarak ticari düzenleme süreçlerinde daha fazla bağlantı elde etmenin yollarını keşfetmek için Hollanda Gümrük İdaresi ile görüşmeler devam etmektedir. [34]

7. ÖNERİ

Elektronik Gümrük İşlemleri Dairesi Blokzincir Platformu (EBP)

Karayolu taşımacılığı ile 4000 serbest dolaşıma giriş rejimi kapsamı beyanname işlemi, akıllı sözleşme/chaincode ihtiva eden Blokzincir ağı ve yurtdışı ihracatçı ülke gümrük idaresi, Ticaret Bakanlığı, serbest dolaşıma giriş işlemi süreçlerine dâhil olan kurumlar ve dış ticaret sürecinin taraflarının API' ler (iki uygulamanın birbiriyle konuşmasına olanak tanıyan bir yazılım aracısı olan Uygulama Programlama Ara yüzü) kullanılarak EBP' ye bağlanması ile yapılabilir.

Adımlar:

1- Yurtdışı ihracatçı ülke gümrük idaresi; ihracatçı beyanında yer alan kıymet, ihracatçı, ithalatçı, nakliyeci, kalem, kap, kilo veya adet bilgilerini EBP' ye gönderir.

2- Nakliyeci; taşıma aracı, hareket saati, sınır gümrük idaresi ve varış gümrük idaresi bilgilerini EBP' ye gönderir.

3- Sınır gümrük idaresi; taşıma aracının araç bilgisini, mühür numarasını, ülkeye giriş saatini ve sınır gümrüğünden çıkış saatini EBP' ye gönderir.

4- Nakliyeci veya nakliye işleticisi; ithalat gümrük idaresine varış saatini ve araç bilgisini EBP' ye gönderir.

5- Ambar memuru; taşıma aracının araç bilgisini ve mühür numarasını EBP' ye gönderir.

6- İthalatçı; BİLGE Sistemini kullanarak ithalat beyannamesi oluşturur ve tescil edilmemiş konumdaki beyanname bilgilerini EBP' ye gönderir.

7- EBP; fatura, ihracatçı, ithalatçı, nakliyeci, kalem, kap, kilo veya adet, mühür numarası ve araç bilgilerinin doğruluğunu kontrol eder, ilgili kurumların veri tabanından ithalatçının belge kontrolünü yapar ve sonucu BİLGE Sistemine gönderir.

8- BİLGE Sistemi; beyannameyi teslim alınmış konuma ilerletir ve beyannamenin konum bilgisini EBP' ye iletir. Beyanname kırmızı hatta ise muayene memuru eşyanın fiziki kontrolünü yapar ve kontrol sonucunu EBP' ye iletir.

9- EBP; vergi miktarı ve ödeme talebini bankaya bildirir.

10- Banka; ödendi bilgisini EBP' ye bildirir.

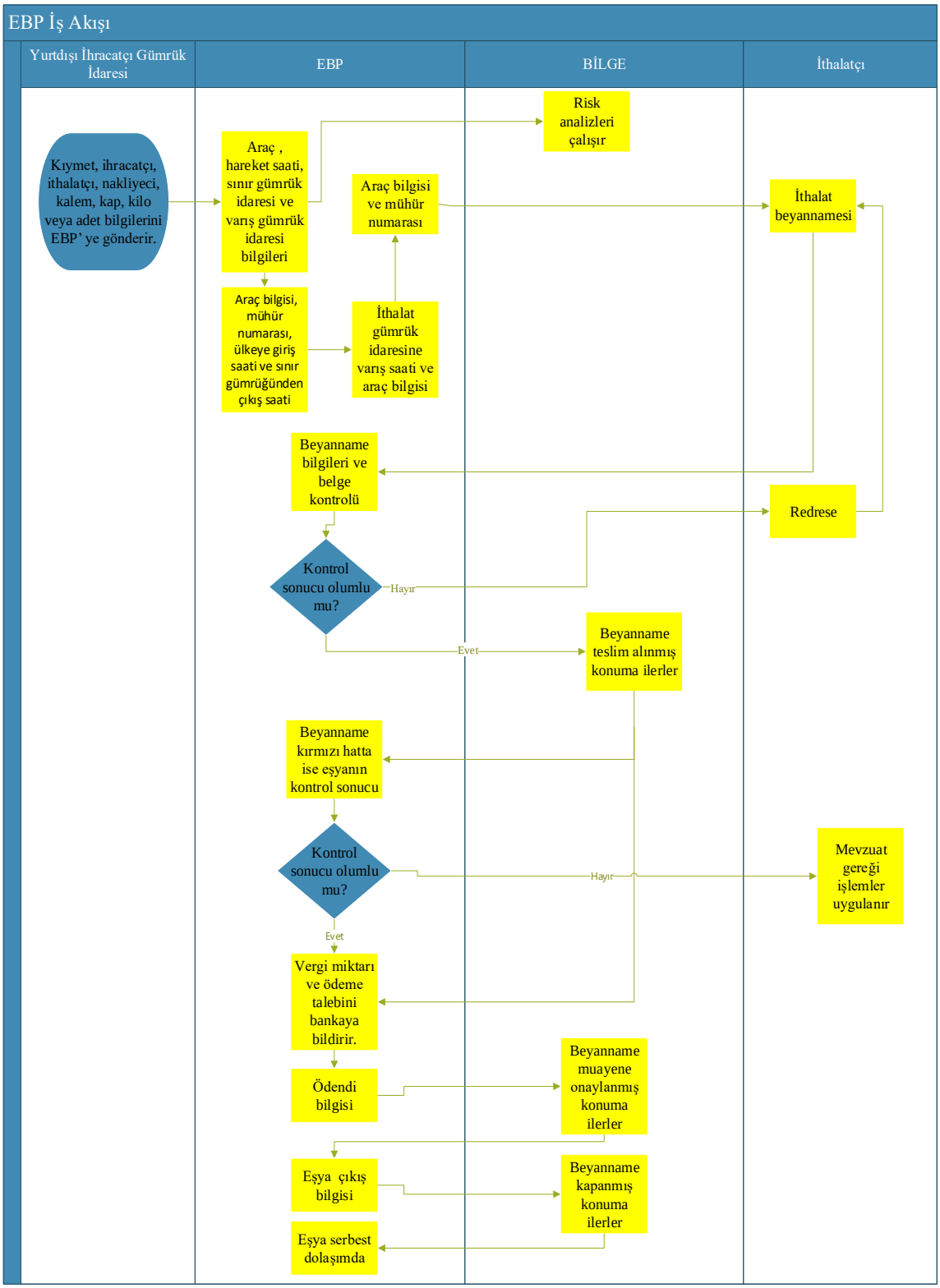
11- EBP; vergi ödendi bilgisini BİLGE Sistemine bildirir.

12- Bilge Sistemi; beyannameyi muayene onaylanmış konuma ilerletir ve beyannamenin konum bilgisini EBP' ye iletir.

13- Ambar memuru; eşya çıkış bilgisini EBP' ye bildirir.

14- EBP; eşya çıkış bilgisini Bilge Sistemine gönderir.

15- Bilge Sistemi; beyannameye ait eşyanın tamamı çekildiğinde beyannameyi kapanmış konuma ilerletir ve beyannamenin konum bilgisini EBP' ye iletir.



Şekil 33:EBP iş akışı

Yukarıda verilen adımlar ve akış şemasına bakıldığında, hali hazırda yerine getirilen serbest dolaşıma giriş rejimi kapsamı beyanname işlemlerinden farklı olarak;

- Özet beyan verilmeyecek,
- Varış bildirimi verilmeyecek,
- Gümrük idaresi personeli tarafından belge kontrolü yapılmayacak(sadece kırmızı hattaki eşyanın kontrolünü yapacak),
- İthalatçı, Tek Pencere Sistemi (TPS) kullanarak izin belgesi almayacak,
- Vergi ödeme işlemi ithalatçı tarafından yapılmayacaktır.

EBP; yazılımındaki Blokzincir teknolojisi ile serbest dolaşıma giriş rejimi kapsamı beyanname işlemine tabi tutulan eşyanın, yurtdışı ihracatçı gümrük idaresinden başlayarak ülkemizde serbest dolaşıma girinceye kadarki sürecinin, bilgisayar veya diğer akıllı aygıtlar kullanılarak bir ara yüz vasıtasıyla takip edilmesini sağlayacaktır. Bu takip, eşyanın serbest dolaşıma giriş süreçlerinin şeffaflığını sağlayacaktır.

Platform, akıllı sözleşme/chaincode sayesinde; dış ticaret sürecinin taraflarının serbest dolaşıma giriş rejimi kapsamı beyanname işlemine konu kıymet, ihracatçı, ithalatçı, nakliyeci, kalem, kap, kilo veya adet beyanlarının uyumlu olup olmadığını kontrol edip ithalatçının hali hazırda Tek Pencere Sistemi (TPS) üzerinden başvuru yoluyla temin ettiği belgelerin, ilgili kurumların veri tabanlarından kontrolünü yaparak işlemlerin devam etmesine izin verecektir. Bu kontroller sayesinde;

- Eksik kıymet beyanından kaynaklı vergi kaybı ortadan kalkacak,

- İthalatçı beyanının doğruluğu kanıtlanacak,

- İthalatçı, gümrük idaresine belge sunmayacak olup el ve göz ile kontrole ihtiyaç duyulmayacak (kırmızı hatta düşen eşyanın muayene memurunca kontrol edilmesi hariç),

- Eşyanın serbest dolaşıma girişine ilişkin olarak ithalatçının ilgili kurumlardan temin etmesi gereken belgeler EBP tarafından kontrol edilerek hem söz konusu belgelerin doğruluğu kanıtlanmış hem de ithalatçının vakit kaybı önlenmiş olacak,

- İşlemlerin kâğıtsız olarak yapılması sebebiyle zaman tasarrufu sağlanacak ve maliyetler azalacak,

Son olarak; söz konusu eşyaya ilişkin vergi miktarı ve ödeme talebi EBP tarafından ilgili bankaya bildirilecek olup ödeme işleminden kaynaklı hatalar ortadan kaldırılacaktır.

EBP' nin sınırlılıkları;

- Ticaret yapılan diğer ülke gümrük idarelerinin Blokzincir ağına dâhil olmaması
- Diğer ülke gümrük idarelerinin hatalı veya eksik bilgi paylaşması
- Serbest dolaşıma giriş rejimi kapsamı beyanname işlemi süreçlerinde yer alan ilgili kurumların Blokzincir ağına dâhil olmaması olarak sıralanabilir.

EBP; hiçbir merkezi sisteme bağlı olmadan çalışabilen, dışarıdan müdahalelere karşı gerekli önlemlerin alındığı, altında yatan güçlü şifreleme teknikleri yardımıyla mutabakat üzerine kurulu şekilde veriyi kayıt altına almakta, kaydedilen veriyi tüm kullanıcılara birer kopyasını dağıtarak saklamaktadır. Bu yapısı ile EBP, platformun taraflarına güven vermektedir.

Karayolu taşımacılığı ile 4000 serbest dolaşıma giriş rejimi kapsamı beyanname işlemi için önerilen EBP; tüm gümrük rejimi kapsamı beyannamelere de kolaylıkla uyarlanabilir.

8. SONUÇ VE DEĞERLENDİRME

Blokzincir; merkezi olmayan doğrulama sistemine sahip, kayıtların birbirine kriptografik elementlerle bağlı olduğu dağıtık bir veri tabanıdır. Veriler sisteme entegre olan kullanıcılar tarafından depolanmaktadır. Blokzincir, sadece finans sektörü ile sınırlı kalmayıp finans dışı sektörlerde de kullanımı günden güne yaygınlaşan bir teknolojidir.

Bünyesinde ihtiva ettiği Akıllı Sözleşmeler ile bulunduğu ağ üzerinde oluşturulan bloklarda yer alan verilerin, önceden belirlenmiş durumları sağlaması halinde otomatik olarak çalışarak önceden tanımlanan görevleri yerine getirmektedir.

Dünya çapında çok sayıda ülkede ve çeşitli sektörlerde giderek artan bir kullanıma sahip olan Blokzincir teknolojisi, gelecek yıllara etkileri yönünden internet ile benzerlik taşımakta olup teknolojinin yakın gelecekte dünyayı teknolojik olarak dönüştüreceği düşünülmektedir.

Bu bağlamda; ticarette zaman ve maliyetten kazanmak, süreçleri hızlandırmak, evrak prosedüründen kurtulmak, zincir üzerindeki tüm verilerin kontrol edilmesi suretiyle yanlış beyanın önüne geçmek, süreçlerin akıllı sözleşmeler vasıtasıyla yürütülmesini sağlamak amacıyla, ticaret süreçlerine dâhil olan tüm tarafların, Bakanlığımız kontrolündeki Blokzincir teknolojisini kullanmasının ticaret süreçlerine olumlu katkıda bulunacağı düşünülmektedir.

KAYNAKÇA

[1] A. USTA ve S. DOĞANTEKİN, Blockchain 101, İstanbul: Bankalararası Kart Merkezi, 2017.

[2] K. DOĞAN ve S. ARSLANTEKİN, «Büyük veri: Önemi, yapısı ve günümüzdeki durum,» *DTCF,* cilt 56, no. 1, pp. 15-36, 2016.

[3] M. ORAL ve M. FURAT, *Veri Saklama Yöntemleri: Sayısal Görüntülerin Damgalanması, Amaçları ve Uygulama Alanları,* 2007, p. 1.

[4] «Türkçe Bilim Terimleri Sözlüğü,» Türkiye Bilimler Akademisi.

[5] Bulut Bilişim, Ankara: Bilgi Teknolojileri ve İletişim Kurumu, 2013.

[6] M. KINACI, *BLOCKCHAIN TEKNOLOJİSİ VE AKILLI SÖZLEŞMELERİN YAYGINLAŞMASININ ÖNÜNDEKİ ENGELLER,* İstanbul, 2019, p. 10.

[7] İ. S. KARAKÖSE, *ELEKTRONİK ÖDEMELERDE BLOK ZİNCİRİ SİSTEMATİĞİ VE UYGULAMALARI,* Kayseri, 2017.

[8] M. ALDEMİR, *Elektronik Para ve Blockchain'in Finansal Yönetim Üzerine Etkileri,* İstanbul, 2018.

[9] A. ÇARKACIOĞLU, «Kripto-Para BITCOIN,» Sermaye Piyasası Kurulu Araştırma Dairesi, 2016.

[10] A. M. Antonopoulos, Mastering Bitcoin, O'REILLY, 2014.

[11] D. L. K. Cuen, DIGITAL CURRENCY, Elsevier, 2015.

[12] T. B. İ. G. Müdürlüğü, «Blokzincir Uygulamalarına İlişkin Kavramsal Çerçeve,» Ankara, 2019.

[13] B. ÜZER, *Sanal Para Birimleri,* Ankara, 2017.

[14] K. Szczepanski. www.thoughtco.com. [Erişildi: Ağustos 2019].

[15] S. BAKTAŞ. www.medium.com. [Erişildi: Ağustos 2019].

[16] C. ÇAVUŞOĞLU, *Elektronik Paranın Gelişimi ve Merkez Bankası Bilançosu ile Para Politikası Uygulamaları Üzerine Etkisi,* Ankara, 2015.

[17] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008.

[18] D. Schwartz, N. Youngs ve A. Britto, *The Ripple Protocol Consensus Algorithm,* 2014.

[19] *Malta:Destination Blockchain İsland.*

[20] www.e-estonia.com. [Erişildi: 19 Ağustos 2019].

[21] www.britishblockchainassociation.org . [Erişildi: 19 Ağustos 2019].

[22] www.fintechnews.ae. [Erişildi: 19 AĞUSTOS 2019].

[23] www.cointelegraph.com. [Erişildi: 19 Ağustos 2019].

[24] www.bctr.org. [Erişildi: 21 Ağustos 2019].

[25] www.bctr.org. [Erişildi: 4 Temmuz 2019].

[26] www.bctr.org. [Erişildi: 28 Şubat 2019].

[27] www.bctr.org. [Erişildi: 16 Nisan 2019].

[28] www.chinadaily.com.cn. [Erişildi: 20 Ağustos 2019].

[29] www.cointelegraph.com. [Erişildi: 28 Temmuz 2019].

[30] www.iccwbo.org. [Erişildi: 21 Ağustos 2019].

[31] www.rbcits.com. [Erişildi: 15 Ağustos 2019].

[32] TradeLens, Solutıon Brıef Edition two.

[33] www.turkishtimedergi.com. [Erişildi: 20 Ağustos 2019].

[34] www.ntp.gov.sg. [Erişildi: 24 Ağustos 2019].

[35] *Media Release,* Singapore Customs, 2018.

[36] *Fact Sheet,* Singapore Customs, 2018.