T.C.
SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BSM 498 BİTİRME ÇALIŞMASI

BLOCKCHAİN İLE MAĞAZA KARTLARINDAKİ PARA TRANSFERİ

G141210067 – Mesut Cem YILDIZ
G131210018 – Ufuk ERDOĞAN
G151210102 – Yasin AYVAZ

Fakülte Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ
Tez Danışmanı : Dr. Öğr.Üyesi Mustafa AKPINAR

2019-2020 Güz Dönemi

T.C.
SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BLOCKCHAİN İLE MAĞAZA KARTLARINDAKİ PARA TRANSFERİ

BSM 498 - BİTİRME ÇALIŞMASI

G141210067 – Mesut Cem YILDIZ
G131210018 – Ufuk ERDOĞAN
G151210102 – Yasin AYVAZ

Fakülte Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ

Bu tez .. / .. / … tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

…….	…….	…….
Jüri Başkanı	**Üye**	**Üye**

ÖNSÖZ

Günümüzde teknolojinin hızla gelişmesi kullandığımız paralar konusunda da birçok yeniliği beraberinde getirmektedir. Lidyalıların parayı bulmasından günümüze kadar gelen süreçte paranın birçok formunu görme şansımız oldu. 90'lı yıllardan itibaren de sanal paraların temelleri atılmaya başladı. Bu sanal paraların asıl patlaması ise 2009 yılında Satoshi Nakamoto isimli biri veya bir grubun yayınladığı manifesto ile olmuştur. BlockChain modeli ile hayatımıza giren Bitcoin günümüzde en çok kullanılan sanal para birimidir. Bitcoin'in çıkışı ve tüm dünyada bu kadar meşhur olmasıyla benzer para birimleri de ortaya çıkmıştır. Bu çalışmada da kullanmış olduğumuz Ethereum ise onlardan biridir.

Bankacılık, eğitim, müzik, eğlence vb birçok alanda kullanılan bu blockchain yapısının adının önümüzdeki yıllarda daha sık duyulması beklenmektedir. Özellikle finans sektöründe sıkça kullanılmaya başlayan bu yapı için birçok banka raporlar yayınlamaktadırlar.

Bu proje kapsamında ERC20 token standardı ve Solidity ile akıllı sözleşmeler yazılarak Ethereum tokenı yaratılmış ve üzerinden kalabalık para transferleri gerçekleştiren bir web sitesi oluşturularak sistemin daha iyi anlaşılması hedeflenmiştir.

Bitirme çalışmamızı hazırlarken bizlere her anlamda destek veren Sn. Dr. Öğr. Üyesi Mustafa AKPINAR hocamıza teşekkürü borç biliriz.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

BTC	: Bitcoin
ETH	: Ethereum
XRP	: Ripple
USDT	: Tether
LTC	: Litecoin
TRX	: TRON
PoW	: Proof of Work
PoS	: Proof of Stake
DApps	: Decentralized Applications

ŞEKİLLER LİSTESİ

ÖZET

Anahtar kelimeler: Sanal Para, BlockChain, Bitcoin, Ethereum, Solidity

Bu proje kapsamında günden güne kullanım alanları oldukça artan Bitcoin, Ethereum v.b. kripto paralar ve Blockchain yapısı model alınarak, bir şirket içinde çalışan insanların maaşları, yol giderleri ve ekstra kazançları gibi ödemeler bu sistemle gerçekleştirilmiştir. Klasik ödeme yöntemlerinin aksine Blockchain yapısında merkezi olmayan bir sistem kullanılmaktadır. Para transferleri gibi işlemlerin kayıtları milyonlarca insanın bilgisayarında aynı anda tutularak saldıralara karşı da yüksek derecede güvenlik sağlanmaktadır.

Günümüzde yayın olarak kullanılan bazı kripto paralar hakkında bilgiler verilmiş ve bunlar arasında en çok karşılaşılan para birimleri olan Bitcoin ve Ethereum'un USD ve TL cinsinden değerleri grafiklerle gösterilerek bu paraların öneminin iyice anlaşılması sağlanmıştır.

Bu kripto paraların bu kadar popüler gelmesinin ana sebebi ise kullandığı BlockChain altyapısıdır. Bir veri tabanı ile arasındaki fark ise BlockChain'de ki verilerin silinemez ve değiştirilemez oluşudur. Tüm kayıtlar herkese açık olduğu için bu kayıtlar herkes tarafından görüntülenebilmektedir.

Üçüncü bir kişiye gerek kalmadan para transferlerinin güvenli ve şeffaf bir şekilde sağlanması ise akıllı sözleşmeler ile sağlanmaktadırlar. Bu akıllı sözleşmelerle birlikte iki taraf için de sözleşme şartları belirlenir ve daha sonra bu şartlar BlockChain sistemine girmek üzere kod yapısına dökülür. Aktif olan bu sözleşme dağıtık bir yapıda saklanır ve korunmuş olur.

Ethereum sanal makinesini hedefleyen akıllı sözleşmeler yazmak için üç tane nesne yönelimli programa dili mevcuttur. Bunlar Solidity, Serpent ve LLL'dir. En sık kullanılan dil ise Solidity'dir. Proje'de akıllı sözleşmeler yazmak için Solidity dili kullanılmıştır.

Bu bağlamda sanal para ve blockchain teknolojisinin getirdiği yenilikleride göz önünde bulundurursak projemizde blockchain üzerinde kalabalık bir satış akıllı sözleşmesiyle konuşacak bir ICO web sitesi oluşturulmuştur. Bu müşteri taraflı web sitesi, kullanıcıların kalabalık satışında token satın alabilecekleri bir forma sahiptir. Projemizde Ethereum tabanlı bir blockchain altyapısı kullanılmıştır. Projeyi farklı sanal makinelerde yayına alıp, birbirleri ile konuşmalarını sağlaması amaçlanmıştır. Proje yapılırken token üreten, kalabalık token alış satışlarını gerçekleştiren ve token dağıtımlarını yapan akıllı kontratlar oluşturulmuştur.

BÖLÜM 1. GİRİŞ

Dijital bir para olan kripto paraların maddi bir karşılığı olup fiziksel gerçekliği yoktur. Sanal para ve BlokChain uygulamaları gerek güvenilir olması gerekse finansal yeniliklere sahip olması itibariyle kullanıcılar için vazgeçilmez bir uygulama haline dönüşmüştür. Sanal paralar reel para piyasasının çalışma düzeninden farklı olduğu için otoriteler tarafından ortak bir tanım altına alınamamıştır. 2014 yılında Avrupa Bankacılık Otoritesi'nin tanımına göre sanal para; "Bir merkez bankası veya kamu otoritesi tarafından ihraç edilmediği halde, doğal olarak veya yasal kişiler tarafından ödeme, transfer, saklama ve elektronik transfer şekli için kabul gören, karşılığının olması da şart olmayan değerin dijital temsilidir." [1]. Sanal para ile ödeme kabul eden büyük teknolojik şirketlerin başını Dell ve Microsoft çekmektedir. İnsanlar e-ticaret şirketlerinin birçoğundan sanal para ile online ödeme yaparak bilgisayarları için donanım ve yazılım satın alabilmektedir. Sanal paralar 'gift card'a çevrilerek Amazon gibi mağazalarda da kullanılabilir.

Bizim çalışmamızda da yeni bir token oluşturulup şirket çalışanları için mağaza parapuanlarının transferi ve satışının gerçekleştirilmesi hedeflenmiştir. Bu çalışmayı yürütürken Ethereum altyapısı kullanılmıştır. Ethereumun kendi sanal makinesini hedefleyen akıllı sözleşmeler yazılabilen, açık kaynak koda sahip, halka arz etmiş ve BlockChain altyapısını kullanan, merkezi olmayan bir bilgi işlem platformu olması Ethereum altyapısını seçmemizin nedenlerinden bazılarıdır. Çalışmamızda kullanacağımız ERC20 token standardı bize oluşturacağımız akıllı sözleşmeler için bir arayüz sağlamaktadır.

Proje dökümanımızın diger bölümlerinde sırasıyla; kripto para kavramı, kripto paranın kullanım alanları, BlockChain altyapısı, Ethereum altyapısı, önerilen model ve proje bölümleri yer almaktadır.

Kripto Para Kavramı

Kripto para hayatımıza ilk olarak 2008 yılında Satoshi Nakamoto isimli birinin veya bir grubun yayınladığı açıklayıcı metniyle girmiştir. Daha önce de üzerinden çalışmalar sürdürülen kripto paralar, blok zinciri yapısını kullanan ilk kripto para olan Bitcoin ile şu an tüm dünyada yatırımcılarına çokça para kazandırmakta ve bu teknolojilerin gelişerek farklı sektörlerde kullanımını sağlamaktadır.

Bitcoin tüm dünyada en çok bilinen kripto paradır. Bitcoin dışında yaklaşık 3000'den fazla kripto para mevcuttur. 2008 yılından itibaren ciddi bir finansal sistem haline gelmiştir. Ülkemizde ise 2017 yılından sonra daha da önemli bir hale gelmeye başlamıştır.

Kripto paralar bildiğimiz ödeme yöntemlerine bir alternatif olan bir para birimi olarak ortaya çıkmıştır. İnsanlar ödemelerini Bitcoin veya diğer kripto paralar ile yapabildiklerini farkettiklerinde bu paraların kullanım alanları oldukça genişlemiştir.

Sanal Paranın Kullanım Alanları

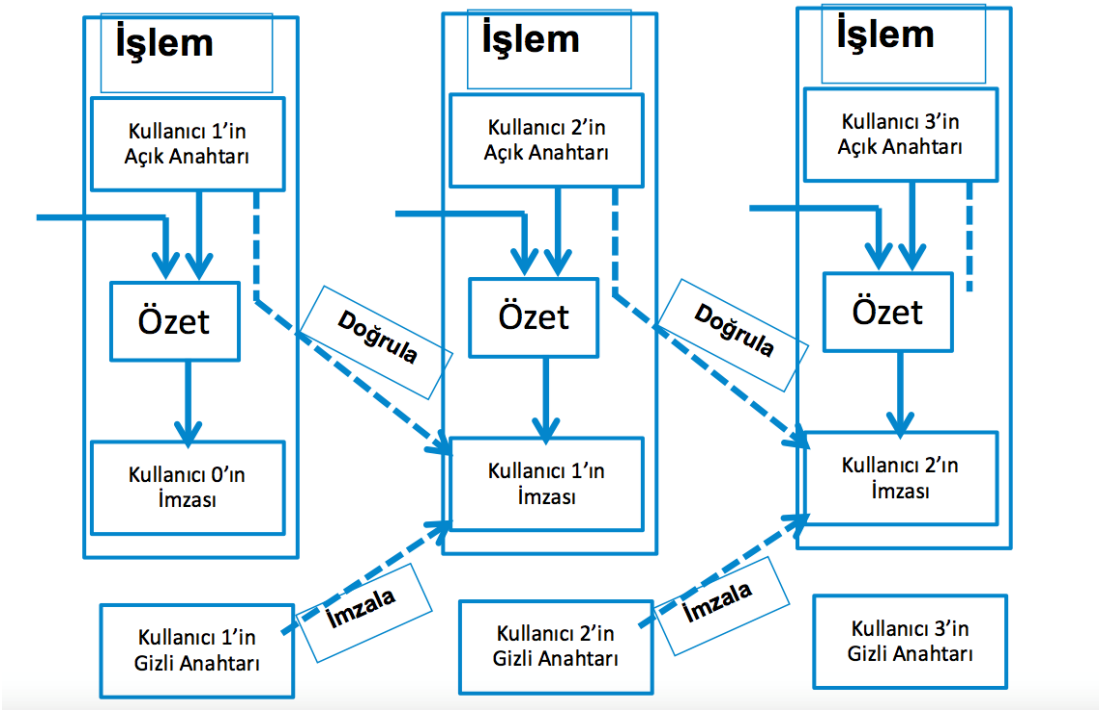
Dünya genelinde günden güne kullanımı artan bu sanal paraların kullanım alanları ise oldukça geniştir. Birçok online alışveriş sitesi başta Bitcoin olmak üzere sanal paraları kabul etmektedirler. Örnek olarak Bitpay hesabı açarak Bitcoin ödemeleri gerçekleştirilmektedir.

Dünyanın en önemli şirketlerin olan Microsoft, Dell vb. şirketler Bitcoin ödemelerini kabul etmektedirler. Ülkemizde bu kadar yaygın olmasada Amerika başta olmak üzere birçok ülkede sanal paraların kullanım alanları oldukça geniştir. Bitcoin ve benzeri kripto paralar kullanılarak restoran ve barlar dahil olmak üzere birçok alanda ödemeler gerçekleştirilebilmektedir. Aynı zamanda ülkemizde genel olarak finans ve e-ticaret sektörlerinde yaygın olarak kullanılan bu para birimleri dünyada ise oyun, müzik, eğitim ve nesnelerin interneti gibi alanlarda da oldukça sık kullanılmaktadır.

1.3. BlockChain

BlockChain Bitcoin, Ethereum vb. kripto paraların var olabilmesi için yaratılmış bir altyapı ve merkezi olmayan veri kayıt sistemi olarak tanımlanabilmektedir. Hiç bir aracıya ihtiyaç duymadan para transferleri ve birçok alanda kullanabilen bir zincirleme sistemidir. Bir veri tabanı ile arasındaki fark ise blockchaindeki verilerin silinemez veya değiştirilemez oluşudur. Bu veriler milyonlarca bilgisayar üstünde saklanmaktadır. Bu sayede bilgisayar korsanı ve kötü niyetli yazılım gibi tehditlere karşı güvenlik çok üst düzeye çıkmış olmaktadır.

Her blok zinciri bir başlangıç bloğuna ihtiyaç duymaktadır. Bu ilk bloğa genesis bloğu ismi verilmektedir. Her blok kendisinden önceki bloğun hashlenmiş haline sahiptir ve bu şekilde zincir yapısı sağlanmaktadır. Zincire en son eklenen blok ağdaki tüm bilgisayarlara gönderilerek kaydı tutulmuş ve güvenliği sağlanmış olur. Aşağıdaki şekilde yukarıda anlatılan blok zinciri yapısı görülmektedir.



Şekil 1.1. Blok Zincirinde Bir Bloğun Yapısı

1.4. Sanal Para Birimleri

2008 yılında Amerika'da yaşanan ekonomik kriz sonrasında ortaya çıkan Bitcoin ve Blockchain kavramları ile birlikte günümüzde 3000'den fazla sayıda kripto para kullanılmaktadır. Genel olarak en yaygın bilinen örnekleri Bitcoin ve Ethereum'dur ve yüzlerce çeşit kripto para birimi başta finans ve e-ticaret sektörü olmak üzere uluslararası piyasalarda kullanılmaktadır. En değerli kripto para birimleri arasında; Bitcoin, Ethereum, Ripple, Tether, Litecoin, EOS, Steller, Tron, Cardano yer almaktadır.

1.4.1 Bitcoin (BTC)

Bitcoin bir kripto para ve ödeme sistemidir. Bu sistem 2008 yılında Satoshi Nakamoto takma adıyla bir kişi veya bir grup tarafından yayımlanan 9 sayfalık bir pdf belgesiyle hayatımıza girmiştir. Bu belgenin başlığı "Kişiden Kişiye Elektronik Para Sistemi." dir [2]. Burdaki kişiden kişiye kelimeleri, merkezi olmayan dağıtık bir ağ yapısına benzetilmektedir. Yani merkezi olmayan bir sistem demektir.

Genel olarak ülkelerin paraları başta ülkelerin merkez bankası olmak üzere, bankalara ve finansal organizasyonlara bağlıdır. Bitcoin dünyasında ise böyle bir merkezi otorite bulunmamaktadır. Onun yerine ise açık kaynak kodlu bir yazılım kullanılmaktadır.

Bitcoin dünyasına ilk girdiğimizde hesap açmamız gerekmektedir. Buna dijital cüzdan da denilmektedir. Birine bitcoin gönderilmek istendiğinde hesap numarası, alıcının hesap numarası ve gönderilen miktar tüm dünyadaki blockchain zincirinde tutulmakta ve senkronize edilmektedir. Bu işlem ve kriptografi sayesinde ise bu paraların güvenliği sağlanmaktadır. Her cüzdanın iki adet anahtarı vardır. Özel anahtar sadece bizim bilip kullandığımız anahtar olarak tanımlanabilir. Para göndermek istediğimizde ilk olarak özel anahtar ile imzalanır ve daha sonra genel anahtar ile bitcoin ağına gönderilir. Ağdaki insanlar ise bu genel anahtara bakarak işlemin doğruluğunu kontrol ederler ve doğruluğu kanıtlanan işlem güvenli bir

şekilde yönetilir. Bitcoin'in Dolar ve Türk lirası karşısındaki değerleri sırasıyla Şekil 1.2 ve Şekil 1.3'de gösterilmiştir.

Şekil 1.2. Bitcoin/USD Grafiği [3]

Şekil 1.3. Bitcoin/TL Grafiği [4]

1.4.2. Ethereum (ETH)

Ethereum 2013 yılında bir Bitcoin Konferansında, şu an kurucusu olarak tanıdığımız Vitalik Buterin tarafından hayatımıza girmiş ve 2019 yılı itibariyle Bitcoin'den sonra piyasadaki en değerli ikinci kripto olmayı başarmış bir para birimidir. Ethereum'da kullanılan para biriminin ismi "ether" olarak adlandırılmaktadır.

Günümüzde birçok coin Ethereum platformu üzerinden gerçekleştirilmektedir. Token olarak ortaya çıkmakta ve daha sonra bu tokenlar Ethereum üzerinden coin olarak işlem görmektedirler. Bunlardan bazıları EOS, TRON gibi coinler Ethereum Blockchainini kullanarak var olmuşlardır. Şekil 1.4 Ethereum'un Dolar karşısında degişimini göstermektedir.

Şekil 1.4. Ethereum/USD Grafiği [5]

1.4.3. Ripple (XRP)

Ripple 2012 yılında Blockchain altyapısını kullanarak para transferi işlemlerini hızlandırmak amaçlı ortaya çıkmış bir kripto paradır. Sembolü XRP olan Ripple şirketi Brad Garlinghouse tarafından yürütülmektedir.

Teknik olarak Bitcoinden birçok farkı vardır. Ripple'ın asıl amacı Bitcoin madenciliğinin aksine, masrafların olmadığı bir platform oluşturmaktır. Bu nedenle ilk ortaya çıktığında 100 milyar Ripple zaten yaratılmıştı. Bu sayede madenciler otomatik olarak saf dışı kaldılar. Her yıl 1 milyar Ripple piyasaya sürülmektedir. Ripple diğer kripto paraların aksine bir şirket tarafından yönetilmektedir ve bu da merkezi olan bir kripto kavramı olarak nitelendirilmesine neden olmaktadır.

Ripple'ın onca sektör arasında odaklandığı tek sektör Bankacılık ve Finans sektörüdür. Ripple ile yapılan para transferi işlemlerinin düşük maliyetli ve hızlı olması nedeniyle bu sektördeki şirketleri her geçen gün kendisine eklemektedir. Merkezi olması nedeniyle de şirketlerin ve bankaların sıkça tercih ettiği bir kripto kavramı olarak piyasada kullanılmaktadır.

1.4.4. Litecoin (LTC)

Litecoin, eski bir Google çalışanı Charlie Lee tarafından 7 Ekim 2011 yılında açık bir kaynak kodlu istemci aracılığıyla github üzerinden piyasaya sürülmüştür. 1 hafta sonra Litecoin ağı hayata geçmiştir. Litecoin blok zinciri yapısında, yeni bir blok oluşturma süresini azaltarak coin sayısını ve farklı karma algoritmaları arttırarak yeni bir arayüzle ortaya çıkmaktadır.

Litecoin Bitcoin'in çalışma prensibinden esinlenerek geliştirilmiştir. Aralarındaki en büyük fark ise Litecoin'in mining algoritmasının kişisel bilgisayarlarda bile sürekli olarak madencilik yapabilme olanağı sağlamasıdır. Aynı zamanda işlemlerin daha çabuk onaylanmasını sağlayan bir teknolojiyi de bünyesinde barındırmaktadır ve diğer kripto paralara nazaran daha fazla depolama imkanı sunmaktadır.

1.4.5. Tether (USDT)

Bitcoin blok zincirinde üretilip dağılan Tether, yirmiden fazla kripto para alım satım platformunda işlem gören bir kripto kavramıdır. Üreticisi Tether Limited tarafından ABD dolarına endeksli bir kripto para olarak tanımlanmıştır.

Tether açık kaynaklı bir protokol olan Omni protokolü üzerindeki 31 numaralı kripto varlıktır. Transfer işlemleri bu protokol ile birlikte Bitcoin Blockchaini üzerine yazılır. Tether daha sonra Ethereum ağında ERC20 kontratı olarak da yayınlanmıştır. Ethereum ağı üzerinden de transfer edilebilir. Bitcoin ve ethereum ağı üzerindeki Tether işlemleri birbirinden bağımsızdır. Bu nedenle ağlar üzerinde karşılık transfer yapılamamaktadır.

Dolara endeksli olduğu için 1 Tether'in değeri için 1 dolar diyebiliriz. Tether'leri saklamak, almak veya göndermek için Omni protokolü destekli cüzdanlar kullanılmaktadır. Omni core Bitcoin Blockchainin tamamını senkronize etmektedir.

1.4.6. Tron (TRX)

Tron küresel dijital eğlence sektörüne hitap eden bir coindir. 2014 yılında Justin Sun tarafından kurulmuş merkezi olmayan bir kripto paradır. Tron'un genel olarak amacı tüm kontrolü kullanıcılara vermektir.

Tron'un 4 adet çalışma prensibi vardır. Bunlardan ilki veri özgürlüğü; her türlü içerik özgür ve herhangi bir kontrol olmadan platforma yüklenebilir, depolanabilir ve dağıtabilir. İkincisi ise içerik sağlamadır: İçerikler sayesinden dijital varlık kazanılarak platform kendi kendine varlığını sürdürebilir. Üçüncüsü Kişisel ICO: Platform üyeleri ICO düzenleyerek geliştirdiği dijital varlığın dağıtımını yapabilir. Son prensip ise altyapıdır: dağıtımlı dijital varlıklara dağıtımlı al sat imkanıdır.

BÖLÜM 2. ETHEREUM

Ethereum 2014 yılında Vitalik Buterin tarafından kurulmuştur. Bitcoin'deki gibi BlockChain yapısından esinlenilerek oluşturulmuştur. İlk bakışta bir "altcoin" gibi nitelendirilsede gerçekte diğer altcoinlere göre daha fazla farklı işlemler içeren bir dijital para birimidir.

Ethereum aynı zamanda kendi sanal makinesi hedefleyen akıllı sözleşmeler yazılabilen, açık kaynak koda sahip, halka arz etmiş ve BlockChain altyapısını kullanan, merkezi olmayan bir bilgi işlem platformudur. Uluslararası bir ortak düğüm kullanarak komut dosyalarını çalıştırabilen merkezi olmayan bir Turing tam sanal makinesi ya da diğer adıyla Ethereum Sanal Makinesi ile işlem görmektedir.

Ethereum şu an da kripto para dünyasında çok büyük bir öneme sahiptir. Geliştirdiği akıllı sözleşmeler sayesinde insanlar kendi coinlerini üreterek halka arz edebilirler. Hali hazırda birçok coin Ethereum platformunu kullanmaktadır. EOS ve TRON gibi coinler buna örnek olarak verilebilir.

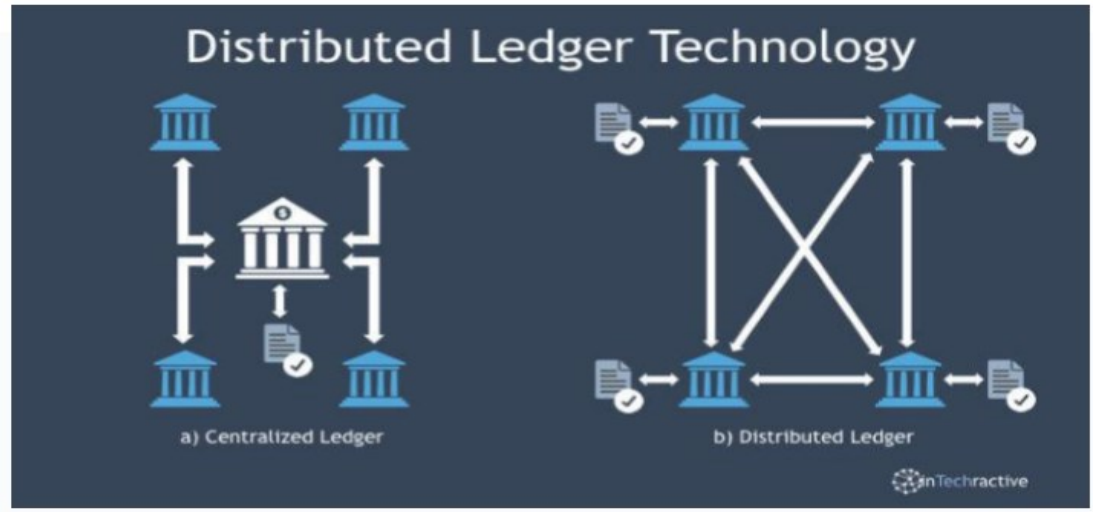
Bitcoin'de ortalama blok süresi yaklaşık 10 dakika iken Ethereum'da ise bu sürenin 12 saniyeye düşürülmesi hedeflenmektedir. Ethereum'un avantajlarından bazıları şunlardır. Değiştirilemezlik; üçüncü taraflar Ethereum platformunda yer alan herhangi bir veriyi değiştiremezler. Uygulamalar fikir birliği ilkesi doğrultusunda oluşturulan gizliliği imkânsız hale getiren bir ağa dayanmaktadırlar. Bu uygulamalar hileli etkinliklere ve siber saldırılara karşı korunmaktadırlar.

2.1. Distributed Ledger Technology Tarihçesi

1991 yılında Stuart Haber ve W. Scott Stornetta adında iki şahıs kriptografi kullanarak şifrelenmiş Blockchain benzeri bir oluşumdan bahsetmişlerdir. Projeleri dijital bir dökümanın zaman damgalamalarının değiştirilememesi üzerine kuruluydu. 1992 yılında Haber, Stornettave Bayer bu fikir üzerinden çalışmalarını kurumsallaştırma karar vermişler ve Merkle Tree ortaya çıkmıştır. 1998'de Nick Szabo isimli Macar kökenli kriptolog Bilgold adında Bitcoin'e çok benzer bir para biriminden bahsetmiştir. 2002 yılında SecureDLT sisteminden bahseden makale yayınlanmış. İlk Blockchain projesi olarak literatüre geçen Bitcoin, 2008 yılında Satoshi Nakamoto tarafından kavramsallaştırılarak 2009'da hayata geçirilmiştir.

2.1.1. Distributed ledger technology çalışma mantığı

Dağıtık defter teknolojisi fikrinin en bilinen uygulaması kripto paralardır. Kripto para transferlerindeki her işlem kaydı dağıtık bir şekilde Node dediğimiz kayıt defterlerine yazılmaktadır. Bir bankanın muhasebe defterinin şifrelenmiş şekilde birden çok noktada zaman damgalarıyla beraber şifreli tutulduğu düşünülebilir. Yani blockchain'e eklenen verilerin bir kopyası sisteme dahil olarak pek çok bilgisayarda eşzamanlı olarak kaydedilmektedir. Böylece sisteme hizmet eden bilgisayarlardan birkaçının başına bir şey gelecek olsa bile Blockchain'in güncel hali diğer bilgisayarlarda da bulunduğu için herhangi bir kayıp yaşanması söz konusu değildir.



Şekil 2.1. Distributed Ledger Technology [6]

2.2. Merkezi Veritabanları ile Blockchainin Farkları

2.2.1. Merkezi veri tabanları

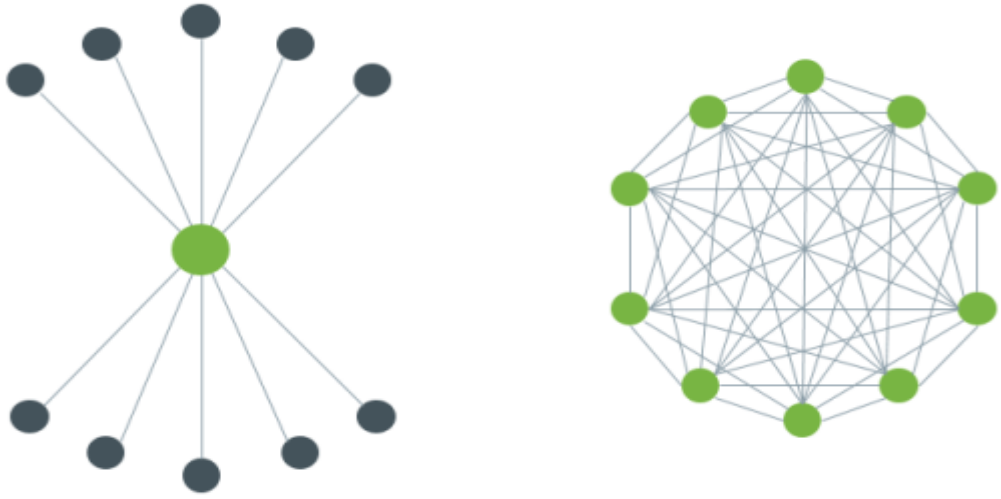
Facebook, Google, Uber, Amazon gibi iş modelleri kendilerine ait sunucularda bizim bilgilerimizi tutarken bu veriler üzerinden gelir modeli oluşturmaktadırlar. Verilerin tamamı bu şirketler tarafından rahatlıkla kullanılabilmektedir.

Müşteri verileri hacklenme durumunda satılabilir bir kaynak olarak hackerları beklemektedir.

2.2.2. Blockchain

Blockchain network ‘üne bağlı tüm bilgisayarlar aynı blockchain veritabanına parçalı veya tüm olarak sahiptirler. Public ledger olduğu için herkes geçmiş işlemlere erişme imkanına sahiptir. Cüzdan adresleri anonimdir.

Hiçbir taraf tek başına veriyi veya bilgiyi kontrol edemez. Her bir node işlem yapacağı tarafla ilgili kayıtları doğrulayabilir ve bunun için bir aracı gerekmez.



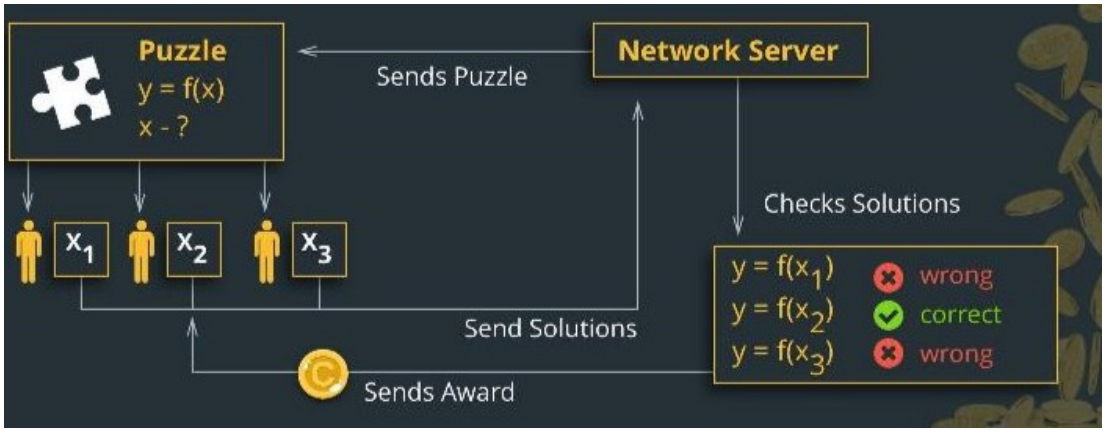
Şekil 2.2. Merkezi ve Dağıtık Veritabanı

2.2.3. BlockChain çalışma mantığı

Her transaction grubuna “block” denilir. Örnek olarak transaction bir cüzdandan bir cüzdana coin transfer işlemidir. Herkese açık bir Blockchainde, herhangi bir insan veri yazabilmekte/okuyabilmektedir. Blockchain üzerindeki verileri okumak ücretsizdir fakat herkese açık bir blockchain deveri tutmanın bir maliyeti vardır. Bu maliyet Ethereum Blockchain’inde “GAS” denen birimle ölçülmekte ve Ether ile ödenmektedir. 1 Gas= 0.008362 Ethereum Networkte spam ve gereksiz veri tutumunun önüne geçmeye yardımcı olmaktadır. Ethereum gibi miningli Blockchain sistemlerinde bir kez yeni bir blok mine edildiğinde, diğer madenciler bilgilendirilir ve yeni bloğu doğrulayıp kendi zincirlerine eklemeye başlarlar. Böylece veri yedekli şekilde şifrelenmiş şekilde saklanır.

2.2.4. PoW blockchain

Mutabakat protokolünün en önemli yönlerinden biri, tüm zincirler tarafından kabul edilen, zincirlere nasıl ve ne zaman ekleneceğine ilişkin kurallardır. Bu şekilde değiştirilemez bir olay zaman çizelgesi oluştururlar. Bu sayede zincirlerin hepsi veri tabanındaki tüm mevcut durumlar üstünde fikir birliğine varırlar. Tüm zincirlerin toplam bilgi sayımsal gücünün en az %51’ine sahip olmadığı sürece sistem manipüle edilemez. Mutabakatı sağlamak için POW ve POS adında yöntemler bulunmaktadır. POW (Proof of Work) iş kanıtı olarak anılan mutabakat, yapbozu bir araya getirmek için saatlerce uğraşmaya benzer fakat bir yapboz doğru şekilde bir araya getirildiğinde, bunu anlamak için şöylesine bir bakmak yeterlidir. İş Kanıtı mutabakatında, bulmacayı çözmek için gereken çabaya İş ve çözüme de İş Kanıtı adı verilir. Bitcoin, Ethereum gibi coinler bu yöntemle yeni blokları oluşturmaktadır. İş Kanıtı’nı kullanan blok zincirleri, zincire eklenecek her bir yeni blok için böyle bir kanıt gerektirir; bu şekilde yeni bloklar yaratmak için İş’in yapılması gerekir. Bu İş sık sık ‘madencilik’ olarak anılır.



Şekil 2.3. PoW BlockChain [7]

2.2.5. PoS blockchain

PoW için harcanan elektriğin artması ve blokların üretilme süresinin uzaması başka alternatifleri düşünmeye itmiştir. Alternatif olarak "Proof of Stake" kavramı ortaya çıkmıştır. Hisse Kanıtı mutabakat protokolü destekçileri, büyük miktar hisse sahiplerinin, yatırımlarını korumak isteyeceğini ve bu nedenle blok üretiminin sorunsuz ve güvenli bir şekilde devam etmesini sağlamak için daha çok Staking yapacağını savunmaktadır. Bu sistemde saldırgan ağdaki hissenin % 51'ini satın almasını gerekmektedir. Saldırganın aldığı pay ne kadar artarsa, fiyat da o kadar artar ve bu hissenin ağa saldırmak için kullanılması, saldırı nedeniyle hisse değeri azalacağı için büyük bir kayıpla sonlanacaktır. Hisse Kanıtı'nın bazı avantajları; İş'in gerekli olmaması, bu sayede daha az enerji harcanması, %51 saldırısının teorik olarak daha pahalı olmasıdır. Hissesi fazla olan cüzdanlar sistemde Consensus'u sağlamak için sık kullanılan cüzdanlardır. Kişi ne kadar çok hisse tutarsa o oranda sistemde doğrulama hakkına sahip olur ve transfer işleminden kesile coin miktarına ortak olur. Dolayısıyla fazla coin tutan kişiler daha çok staking ile gelirleri daha fazla olacaktır.

2.3. Smart Contract

Smart contractlarla alıcı ve satıcının karşı taraftan istediği koşullar tanımlanmaktadır. Bu koşulların iki taraftan da onaylanması sonucu smart contratlarda belirlenen işlemler gerçekleştirilmektedir. Smart kontratlar birer protokol olarak düşünülebilir

[8]. Bu protokol sayesinde taraflar arası anlaşmazlıklar ortadan kaldırılmakta ve önceden belirlenen kural setlerine göre akıllı sözleşmeler imzalanabilmektedir. Smart contractlarda kullanılan kural setleri işlem maliyetini ve güvenlik riskini azaltır. Smart contractlar yaygın olarak Ethereum BlockChain altyapısında kullanılmaktadır. Nasıl ki Blockchain'de tüm veriler her bilgisayarda tutuluyor ve açık ise smart contract dediğimiz yapıda da tüm veriler aynı şekilde tutulur. Ethereum, dijital hizmetlere odaklı çalışan bir altyapı olduğundan akıllı sözleşmeler Ethereum'un önemli niteliklerinden biri haline gelmiştir. Akıllı sözleşmelerin bu derece önemli nitelik olmasının sebeplerinden biri de güvenli bir ortam sunmasıdır.

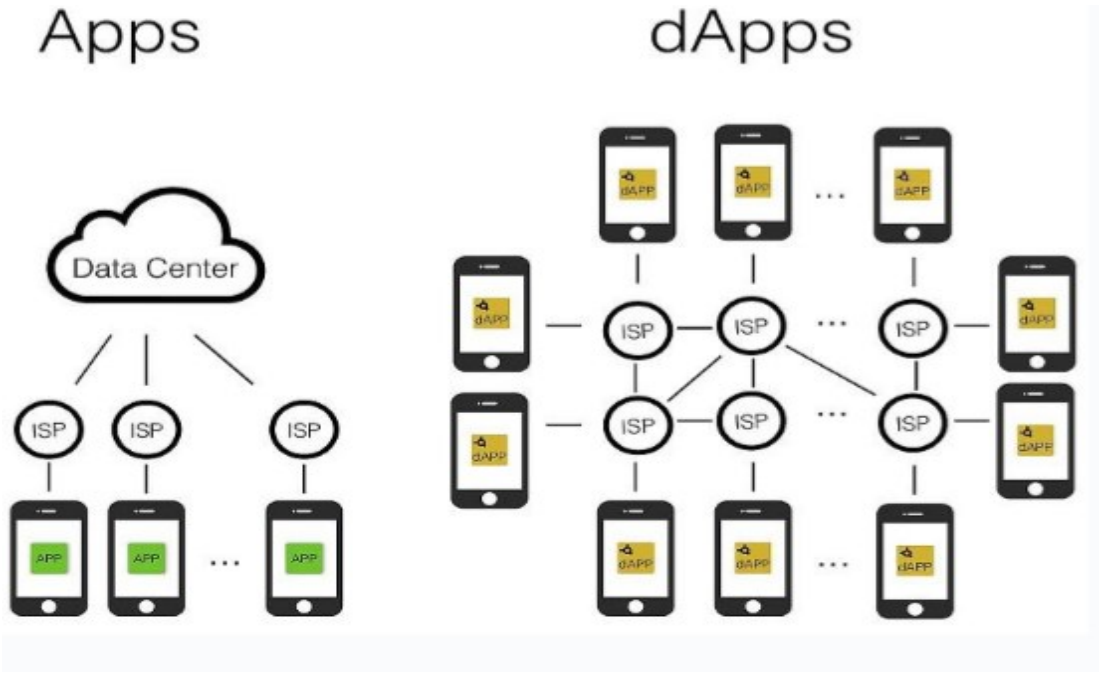
Şekil 2.4. Smart Contract [9]

2.4. Dapps

Merkezi olmayan uygulama anlamın gelmektedir. Örnek olarak Google merkezi bir uygulamadır. Gmail hesabına giriş yapan birinin hangi sunucudan giriş yaptığı bellidir ve bu durum saldırılara açık hale gelmesine neden olmaktadır. Merkezi olmadığı için silinemez ve değiştirilemezler. Bu sebeple saldırılara açık bir durumda değillerdir.

Bir uygulamanın blockchain üzerinde çalışması ve bir DApp sayılabilmesi için aşağıdaki özelliklere sahip olması gerekmektedir.

- Açık kaynak kodlu olma
- Uygulama verilerinin merkezi olmayan halka açık bir blockchain üzerinde tutulması
- Uygulamanın kripto bir token kullanması
- Tokenlerin POW gibi herhangi bir algoritma ile üretilmesi [10].



Şekil 2.5. Dapps [11]

BÖLÜM 3. ÖNERİLEN MODEL

3.1. Projede Yapılacaklar

Blockchain üzerinde kalabalık bir satış akıllı sözleşmesiyle konuşacak bir ICO web sitesi oluşturacağız. Bu müşteri taraflı web sitesi, kullanıcıların kalabalık satışında token satın alabilecekleri bir forma sahip olacaktır. Kullanıcının kaç tane token satın aldığı, tüm kullanıcılar tarafından kaç token satın alındığı ve kalabalık satıştaki toplam token sayısı ve satıştaki ilerlemeyi gösterecektir. Ayrıca, "hesabınız" altında blok zincirine bağlı olduğumuz hesabı da gösterecektir.

Projemizde ethereum tabanlı bir blockchain çözümü kullanılacaktır. Projede farklı sanal makinelerim yayına alınıp, birbirleri ile konuşmalarının sağlanması amaçlanmıştır. Proje yapılırken token üreten, kalabalık token alış-satışlarını gerçekleştiren ve token değıtımlarını yapan akıllı kontratlar oluşturulacaktır.

Projemizi yaparken taraflar arası güven amaçlı, dağıtık bir veri modellemesi ile yeni bir token oluşturulup şirket çalışanları için mağaza para puanlarının transferi ve satışının gerçekleştirilmesi hedeflenmektedir. Projemiz Ethereum tabanlı olduğu için, dışarıdan ether alınabilir ve ether transferi yapılabilir şekilde kurgulanmıştır. Herkes transferleri şeffaf bir şekilde görebilecektir. Bunu sağlayan temel parametre ERC20 token standardıdır.

BÖLÜM 4. KULLANILAN TEKNOLOJİLER VE MODELİN GERÇEKLEŞTİRİLMESİ

4.1. Proje Bağımlılıkları

Projemizi gerçekleştirirken kullanacağımız bağımlılıklar aşağıdaki bölümlerde açıklanmıştır.

4.1.1. ERC-20 token

ERC20, Ethereum'un ağında token'ları yayınlamak için belirli kuralları ve standartları tanımlayan bir protokol standardıdır. Açılımı; ERC, Ethereum Request For Comments'ı, "20" ise bu standardı diğerlerinden ayırmak için benzersiz bir kimlik numarası gibi kullanılmıştır. İnternet için bir HTTP protokolümüz olduğu gerçeğine benzeyecek şekilde, Ethereum yani ERC20'de düzenlenecek tokenler için standart bir protokoldür. ERC20 token srandardını kullanmak bir tokenin aşağıdaki kullanım durumları ile uyumlu olmasını sağlar. ERC20 standardı esasen akıllı sözleşmenin cevap vermesi gereken arayüzü belirler. Akıllı sözleşmenin yapısını ve akıllı sözleşmenin sahip olması gereken işlev türlerini belirtir.

4.1.2. Node package manager (NPM)

JavaScript'in paket yönetici olan Node Package Manager JavaScript geliştirilerinin diğer geliştiricilerle paylaştığı kodların tekrar tekrar kullanılmasını ve yeni uygulamalara kolayca uyarlanmasını kolaylaştırmaktadır. Geliştiricilerden birisi kodunu yeniden ele aldığında, uygulamada yeni geliştirilmiş kodu dahil ederek kolayca güncelleyebilmektedir.

4.1.3. Truffle framework

Ethereum blok zincirinde merkezi olmayan uygulamalar oluşturmamıza izin veren Truffle Framework. Solidity programlama dili ile akıllı sözleşmeler yazmamızı

sağlayan bir dizi araç sunar. Ayrıca akıllı sözleşmemizi test etmemizi ve bunları blok zincire dağıtmamızı sağlar.
Aynı zamanda müşteri taraflı uygulamalar geliştirebilmek için uygun ortamı sağlar. Terminale aşağıdaki komut yazılarak kurulabilir.

```
$ npm install -g truffle
```

4.1.4. Ganache

Bize local(yerel) Ethereum blok zincirimizde 10 hesap verir ve her hesaba 100 sahte ether yüklenmiştir. Truffle Framework web sitesinden indirilebilir.

4.1.5. Metamask

Metamask ethereum blok zincirini kullanabilmemiz için gerekli özel bir tarayıcı uzantısıdır. Local(yerel) blok zincirimizle kişisel hesabımızla bağlanabilmemize yarayan ve yapılan hareketli görebileceğimiz bir ortam sunar. Akıllı sözleşmelerle etkileşim kurulmasına olanak sağlar.

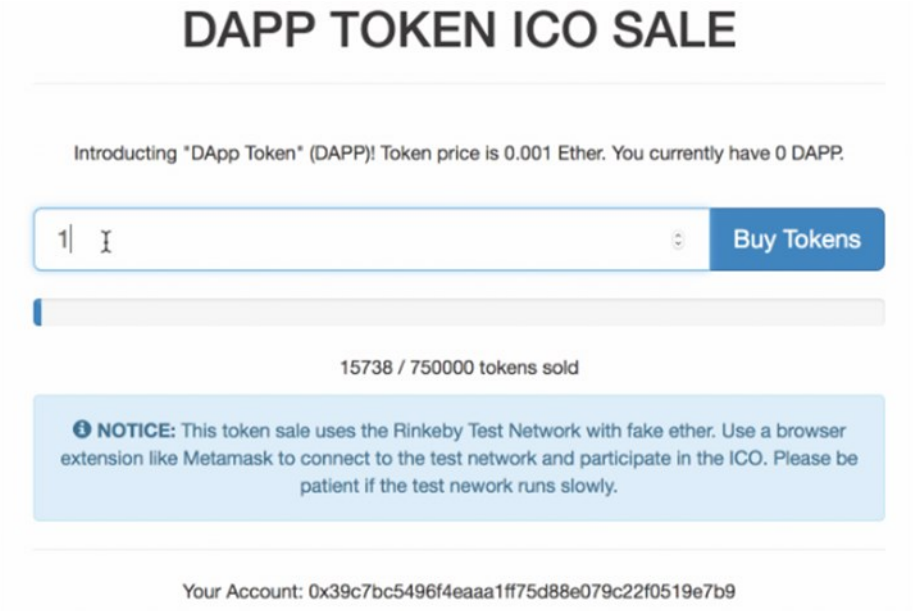
4.2. ERC20 Token Standardı İle Oluşturacağımız Transfer Fonksiyonu

- Token adını ‘string public name = “DApp Token” ‘ olarak saklar.
- Kripto para borsaları için token sembolünü “string public symbol = DAPP” olarak saklar.
- Toplan token arzını “uint256 public totalSupply” olarak saklar.
- Herkesini bakiyesini saklamak için “mapping(address => uint256) public balanceOf” eşlemesini kullanır.
- Kullanıcıları başka bir hesaba token transferi için “transfer” fonksiyonunu kullanır.
- Başka bir hesabın harcamalarını kontrol amaçlı “approve” fonksiyonu tanımlanır ve şayet izin verildiyse “allowance” fonksiyonu yardımı ile günceller.
- Başka bir hesabın token transferine izin veren bir “transferFrom” fonskiyonu tanımlanır.

4.3. Modelin Gerçekleştirilmesi

Projede ERC20 token standardı yardımıyla kalabalık satışlar gerçekleştirebileceğimiz bir web sitesi oluşturuldu. Akıllı bir sözleşmeyle Ethereum token'i oluşturuldu. Projemizde ERC20 token yardımıyla oluşturduğumuz akıllı sözleşmeler, tokenin nasıl çalıştığı ile ilgili tüm davranışları yönetir, token sahipliğini ve hesap bakiyelerini takip eder.

Yukarıda sıralanan işlemler Solidity dili ile yazılan akıllı sözleşme ile yapıldı. Yapılan her işlemi kontrol amaçlı Javascript dili ile birim testler yazıldı. Testler adım adım uygulanarak doğru ve kesin sonuçlar elde edildi.



Şekil 5.1. Dapp Token Ico Sale

BÖLÜM 5. SONUÇLAR VE ÖNERİLER

ERC20 Token standardı ile token (dijital coin) transferi yapan bir web sitesi oluşturduk. Taraflar arası güvenilirlik ilkelerine göre, dağıtık bir mimaride yaptığımız transferler, blok zincir tabanlı Ethererum transferleridir.

Sonuç olarak tokenlerin nasıl çalıştığını ve tokenler yardımıyla nasıl sözleşme oluşturulabileceği, hesabımıza nasıl token ekleyebileceğimiz, eklediğimiz tokenları ve var olan tokenlerımızı nasıl satıp alabileceğimiz gösterilmiştir.

Blockchain altyapısı bize temelde, herhangi bir merkeze bağlı olmadan, kolay, güvenli ve hızlı bir şekilde para transferi yapabilmeyi sağlamıştır.

Özellikle Blockchain teknolojisi ile birlikte yakın gelecekte sağlık sektöründen sigortacılık sektörüne kadar bu sistemin kullanım alanlarının arttığı ve bunun yanında smart contract yapıları ile de alım satım veya kontrat işlemlerini içeren farklı çözümlerin işlemleri kolaylaştırdığı görülmüştür.

Önceden tanımlanmış ve koşullar sağlandığında çalışmak üzere kurulu bekleyen işlemlerin/süreçlerin sunulduğu esnek mimarilerin kullanıma açılması da hayatımıza ilk aşamada girmesi beklenen gelişmeler olarak sıralanabilir. Sonuç olarak Blockchain teknolojisi zaman içinde yaygınlaşarak çeşitlenecektir ve daha farklı alanlarda kullanıma açılacaktır.

KAYNAKLAR

[1] Dr. Murat Dağıtmaç -Nöropsikolog Şehadet Ekmen "Dijital Psikolojik Devrim", 2019

[2] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf , 2008

[3] Bitcoin/USD Grafiği, http://bitcoin.tlkur.com/dolar/5yil

[4] Bitcoin/TL Grafiği, http://bitcoin.tlkur.com/turk-lirasi/5yil

[5] Ethereum/USD Grafiği, https://dovizgrafik.com/kripto/ethereum

[6] Distributed Ledger Technology, https://medium.com/@norachukz/daex-blockchain-the-best-clearing-ecosystem-3e0daa2c19b8

[7] PoW BlockChain, https://coin68.com/li-giai-ve-proof-of-work/

[8] https://teknolojivefinans.com/ak%C4%B1ll%C4%B1-s%C3%B6zle%C5%9Fme-smart-contract-nedir-4a9f74a87452

[9] Smart Contract, https://coil.com/p/cipher/Smart-Contract-What-does-this-blockchain-technology-application-entail-/xmTQ9aN5Y

[10] Süleyman Kaya "Dapps-Merkezi Olmayan Uygulamalar" https://coinbalina.com/dapps/ , 2018

[11] Dapps, https://towardsdatascience.com/what-is-a-dapp-a455ac5f7def

ÖZGEÇMİŞ

Ufuk Erdoğan, 06.05.1995 de İstanbul'da doğdu. İlk, orta ve lise eğitimini Sarıyer'de tamamladı. 2013 yılında Firuzan Kemal Demironaran Lisesi'nden mezun oldu. 2013 yılında Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü'nü kazandı. 2015 yılında Arkas Lojistik Şirketinde donanım stajını ve 2016 yılında da İnnova Şirketinde yazılım stajını yapmıştır. SAÜ Bilgisayar Mühendisliği Bölümünde öğrenim görmektedir.

Yasin Ayvaz, 06.05.1996 da GEYVE' de doğdu. İlk, orta eğitimini Geyve'de lise eğitimini Sakarya Cevat Ayhan Fen Lisesinde tamamladı. 2015 yılında Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü'nü kazandı. 2018 yılında Arvasis Bilişim ve Danışmanlık San. ve Tic. A.Ş. yazılım stajını tamamladı. SAÜ Bilgisayar Mühendisliği Bölümünde 4. Sınıf öğrencisi olarak eğitimine devam etmektedir.

Mesut Cem Yıldız, 22.03.1995 tarihinde Van/Merkez'de doğdu. İlk, orta eğitimini Van'da, lise eğitimini İstanbul Büyükçekmece Atatürk Anadolu Lisesi'nde tamamladı. 2014 yılında Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü'nü kazandı. 2017 yılında Enviyo Bilgisayar Hizmetleri ve Yazılım A.Ş şirketinde yazılım stajını tamamladı. 2018 – Ağustos ayından itibaren Safrantek Bilişim ve Teknoloji Geliştirme Hizmetleri A.Ş.'de aktif olarak DevOps Engineer pozisyonunda çalışmaktadır. SAÜ Bilgisayar Mühendisliği bölümünde 4. Sınıf öğrencisi olarak eğitimine devam etmektedir.

BSM 498 BİTİRME ÇALIŞMASI
DEĞERLENDİRME VE SÖZLÜ SINAV TUTANAĞI

KONU :
ÖĞRENCİLER (Öğrenci No/AD/SOYAD):

Değerlendirme Konusu	İstenenler	Not Aralığı	Not
Yazılı Çalışma			
Çalışma klavuza uygun olarak hazırlanmış mı?	x	0-5	
Teknik Yönden			
Problemin tanımı yapılmış mı?	x	0-5	
Geliştirilecek yazılımın/donanımın mimarisini içeren blok şeması (yazılımlar için veri akış şeması (dfd) da olabilir) çizilerek açıklanmış mı?			
Blok şemadaki birimler arasındaki bilgi akışına ait model/gösterim var mı?			
Yazılımın gereksinim listesi oluşturulmuş mu?			
Kullanılan/kullanılması düşünülen araçlar/teknolojiler anlatılmış mı?			
Donanımların programlanması/konfigürasyonu için yazılım gereksinimleri belirtilmiş mi?			
UML ile modelleme yapılmış mı?			
Veritabanları kullanılmış ise kavramsal model çıkarılmış mı? (Varlık ilişki modeli, noSQL kavramsal modelleri v.b.)			
Projeye yönelik iş-zaman çizelgesi çıkarılarak maliyet analizi yapılmış mı?			
Donanım bileşenlerinin maliyet analizi (prototip-adetli seri üretim vb.) çıkarılmış mı?			
Donanım için gerekli enerji analizi (minimum-uyku-aktif-maksimum) yapılmış mı?			
Grup çalışmalarında grup üyelerinin görev tanımları verilmiş mi (iş-zaman çizelgesinde belirtilebilir)?			
Sürüm denetim sistemi (Version Control System; Git, Subversion v.s.) kullanılmış mı?			
Sistemin genel testi için uygulanan metotlar ve iyileştirme süreçlerinin dökümü verilmiş mi?			
Yazılımın sızma testi yapılmış mı?			
Performans testi yapılmış mı?			
Tasarımın uygulamasında ortaya çıkan uyumsuzluklar ve aksaklıklar belirtilerek çözüm yöntemleri tartışılmış mı?			
Yapılan işlerin zorluk derecesi?	x	0-25	
Sözlü Sınav			
Yapılan sunum başarılı mı?	x	0-5	
Soruları yanıtlama yetkinliği?	x	0-20	
Devam Durumu			
Öğrenci dönem içerisindeki raporlarını düzenli olarak hazırladı mı?	x	0-5	
Diğer Maddeler			
Toplam			

DANIŞMAN (JÜRİ ADINA):
DANIŞMAN İMZASI: