Özet: Güvenlik sistemlerindeki elde edilen veriler delil niteliğinde verilerdir. Bu verilerin silinme ve değiştirilme tehlikesinden uzak olarak saklanması son derece önemlidir. Bu tehlikelerden uzakta verilerimizi saklamak istediğimizde blockchain felsefesi karşımıza çıkmaktadır. Güvenlik sistemlerinden elde edilen verileri blockchain sistemi ile saklarsak bu tehlikelerden uzakta oluruz. Bu sistemi özel şirketler veya devletler güvenlik sisteminde kullanarak sistemleri güçlü dayanıklı yapabilirler. Bu sistem ile şüphelendikleri kişilerin o tarihler arasında orada olup olmadığının tespitinide çok hızlı gerçekleştirebilecekler.

Bizim makalemizin konusu güvenlik kamera sistemi blockchain ile buluşturmak.

Bu makalede yapay zeka ile kamerada tespit edilen yüzlerin ID’lerinin zaman damgasıyla birlikte blockchain sisteminde verileri depolayan proje anlatılacaktır.

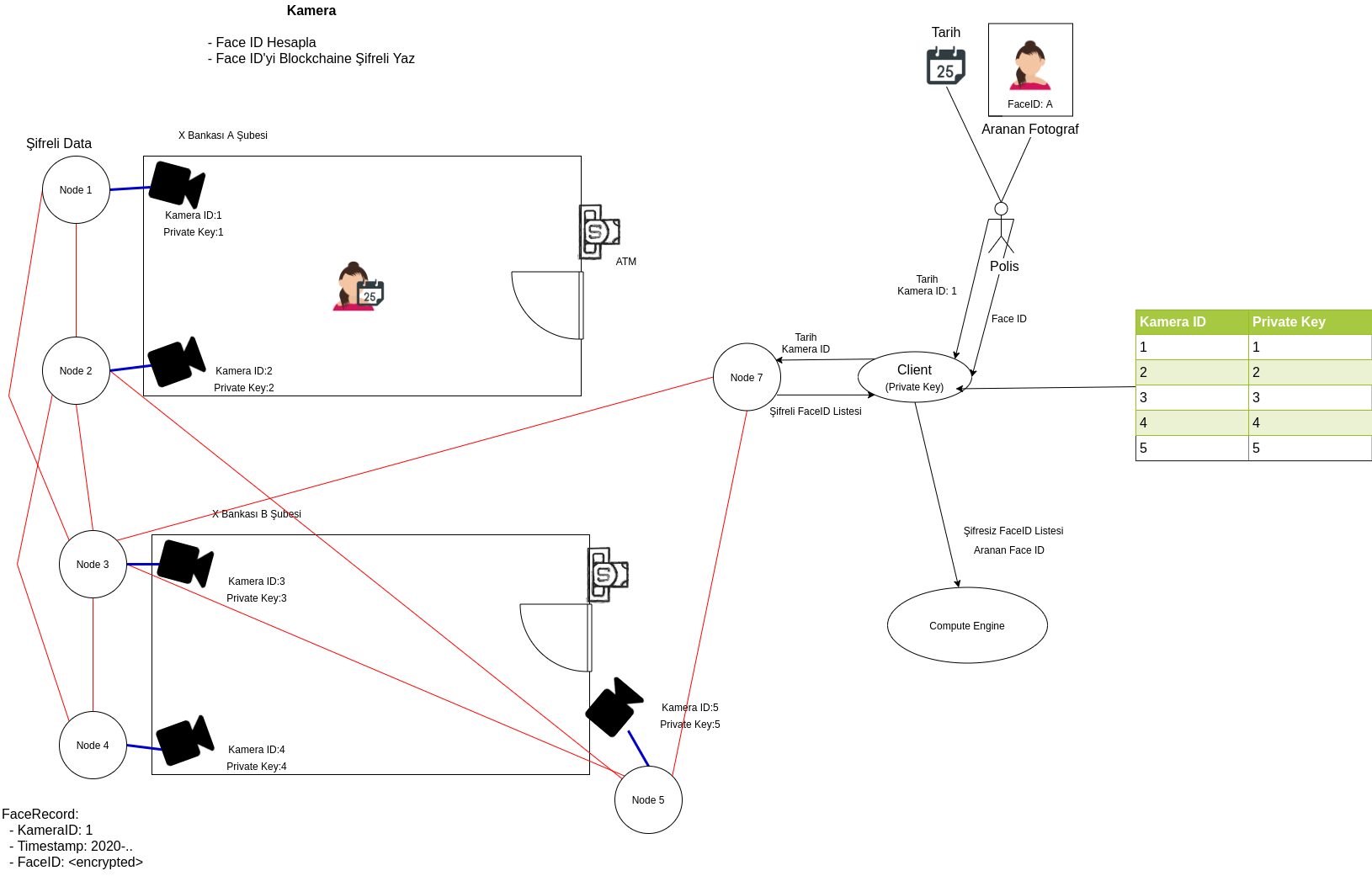
INDEX TERMS Blockchain, Yüz tanıma sistemi, Security System, Criminal Research

Giriş:

Güvenlik sistemleri uzun yıllardır hayatımızda olmasına rağmen sistemleri hala açık ve alt yapıları oldukça basit ve geleneksel. Birçok sorunları mevcuttur. Güvenlik sistemleri merkezi olarak çalıştıklarında o merkeze saldırı yapılırsa güvenlik sistemlerinin kayıt ettikleri dataların hepsini silebilirler veya kameranıza erişim sağlayarak art niyetli faliyetlerde bulunabilirler. Güvenlik sistemlerimizi ademi merkeziyet sisteme geçirirsek kayıtlarımızı ve sistemimizi daha güçlü hale getirmiş oluruz. Kayıtlarımızı daha güvenli ve güvenilir şekilde saklayabiliriz. Bu yeni planlanılan sistemde ihtiyaç duyulan özellik kayıtlarımızın güvenli şekilde saklanması olacak. Kayıtlarımızın hepsi blockchain sisteminde kayıt altında tutulacak bu bize kayıtlarımızın herhangi bir saldırıda silinmemesini ve değiştirilmemesini garanti edecektir.

Bu kamera sisteminde verilerin(yapay zeka ile yüzü tespit edilen kişinin FaceID’si) herkes tarafından görülmesini engellemek için datalar o görüntüleri çeken kameranın private keyi ile şifrelenerek blockchain networkünde saklanacaktır. Böylelikle bu kamera sistemini kullanan kişiler, şirketler veya devletlerin kamera sistemlerinde tespit edilen bu kişiler sistemi kullananların özel bilgileridir. Bu özel bilgilerin yetkisiz kişiler tarafından erişebilmesinin önüne geçilmiş olacak.

Sistemin kullanılması, aranılan kişinin faceidsi ile sistemde önceden tespit edilip kaydedilmiş olan faceidlerin yapay zeka ile eşleşme oranına göre yüksek orandaki kayıtların bilgileri geri döndürülür.Bu sistem sayesinde kamerada birisinin görüntülerinin tespit edilmesi için saatlerce kayıtların izlenmesine gerek kalmıyacaktır.



**Literatür araştırması**

**Blockchain nedir?**

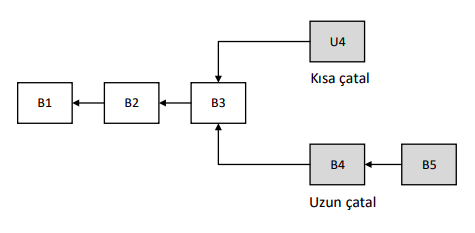
(8) Bloklardan oluşan zincir yapıdaki Blockchain(Blok Zinciri),şifrelenmiş işlem takibini sağlayan dağıtık yapıdaki bir veritabanı sistemidir. Para transferlerinde her adım bir bloğu oluşturur. Örneğin göndericinin adı,gönderilen tutar gibi bilgilerden her biri bir bloktur. Transfer işlemi esnasında oluşturulan bu bloklar şifrelenir,asla değiştirilemez ve kırılamaz hale getirilir. Bu bloklar tüm ağdaki herkese dağıtılır ve herkeste aynı şifreli bilgiler bulunur. Blockchain’ in merkeziyetsizleştirilmiş olma prensibi bu teknolojiye dayanır. Blok üzerindeki bilgiler sadece üzerlerinde belirtilen alıcı ve satıcı tarafından işlenebilir. Bunun yanı sıra Blockchain teknolojisi şeffaftır,isteyen herkes şu ana kadar birikmiş blokları inceleyip onları gözden geçirebilir.

Blockchain teknolojisi bireysel kullanıcılara dijital kimlik üzerinde bugüne kadar benzeri görülmemiş bir kontrol imkanı sağlamaktadır.Dolayısıyla küresel açık bir hesap defteri olan blockchain sadece kripto paraların üretiminde değil birçok farklı alanda saklama, yönetme ve depolama gibi işlemler için kullanılmaktadır. Dijital kimliğe sağladığı imkan onu güven ekonomisinin anahtarı kılmaktadır. Bu açıdan blockchain sadece finans sektörü ile sınırlı kalmamakta, dijital teknolojinin sunduğu imkan işletmeler tarafından da fırsata dönüştürülmektedir. Bu yönüyle blockchain teknolojisinin dördüncü sanayi devriminin merkezinde yer aldığı öne sürülmektedir. Öyle ki önümüzdeki süreçte teknolojinin hayatımızda meydana getireceği büyük etkinin sosyal medya, büyük veri, robotlar ya da yapay zeka ile gerçekleşmeyeceğini ifade eden Don Tapscott gerçek devrimin sanal-dijital paranın temelini oluşturan blockchain olduğunu ifade etmektedir.Blockchain teknolojisi ile farklı sektörlerin teknolojiyle entegre olmasını sağlayan önemli adımlar atılmaktadır.

**Blockchain Türleri:**

(9)

1. İşin İspatı (Proof of Work) İşin ispatı (PoW), Bitcoin ağında kullanılan uzlaşma protokolüdür ve madencilik (mining) olarak adlandırılır. PoW protokolünde daha önceden belirlenmiş özelliklere sahip bir özet (hash) değerine ulaşmak için madenciler karmaşık hesaplamalar yapmaktadır. Belirlenen özet değerine ilk ulaşan madenci zincire yeni bir bloğu eklemeye hak kazanır. İlgili blok hesaplanan özet değeri ile diğer düğümlere yayınlandıktan ve tüm düğümlerden özet değerin doğruluk onayı alındıktan sonra blok zincire eklenir. Daha sonra tüm madencilerin yeni bloğu zincirlerine eklemesiyle zincirin bütünlüğü sağlanmış olur. Bu işlem sonunda bloğu yayınlayan madenci ödüllendirilir.



Şekil 1. Blockzincirin çatallanması

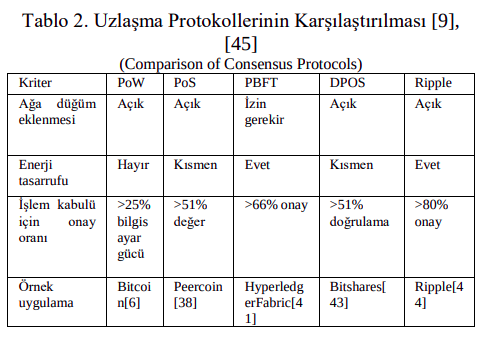
Dağıtık ağ ortamında birden fazla madencinin belirlenen özet değerine aynı anda ulaşması ve aynı anda yayınlaması durumunda blokzincirinde Şekil 1’deki gibi çatallar oluşabilir. Ancak iki rakip çatalın aynı anda sonraki bloğu üretmesi olası değildir. Çatallanma olduktan sonra iki taraftaki madenciler de çalışmaya devam etmektedir. Çatalların birinde yeni bir blok yayınlanınca kısa çataldaki madenciler uzun çatala geçerek burada çalışmaya başlarlar. Örnek olarak Şekil 1’de U4 ve B4 olarak ayrılan iki çatal görülmektedir. B4 deki çatala yeni bir blok olarak B5 eklendikten sonra U4 çatalında bulunan madenciler B çatalına geçerek B6 bloğu için çalışmaya devam edecektir. Madenciler PoW protokolünde çok sayıda bilgisayar gücü gerektiren işlemler yapmak zorunda kalmaktadır. Bu da çok fazla enerji ve bilgisayar gücü gerektirmekte ve zaman kaybına neden olmaktadır. Bu kayıpları azaltmak için içerisinde bazı ek uygulamaları içeren yeni PoW protokolleri geliştirilmiştir. Bunlara örnek olarak matematiksel hesaplamalar için kullanılabilecek özel asal sayı zincirleri üzerine çalışan Primecoin verilebilir

2. Değerin İspatı (Proof of Stake) Değerin ispatı (PoS), PoW protokolüne alternatif enerji tasarrufu sağlayan bir uzlaşma protokolüdür. PoS protokolündeki madenciler bir para miktarının (değerin) sahipliğini kanıtlamak zorundadır. Bu protokolde daha fazla varlık sahibi kişilerin doğrulama işlemlerinde kullanılma olasılığı daha yüksektir. Bu şekilde hesap bakiyesine dayalı tercih çok adil olmamaktadır çünkü tek zengin kişinin ağda baskın olabilmesi mümkündür. PoS protokolünde iyileştirmeler için bir sonraki bloğun yayınlanmasına ilişkin farklı çözümler önerilmektedir. Örnek olarak Blackcoin ile sonraki madenci randomizasyon algoritması ile belirlenmekte ve kombinasyondaki en düşük özet değeri ve varlık miktarını kullanan bir fonksiyon sunulmaktadır. Başka bir örnek olarak Peercoin, varlıkların oluşturulma zamanını dikkate alan bir seçim sunmaktadır. Peercon’ de daha eski ve daha büyük varlık kümelerinin sonraki bloğu oluşturmaları daha olasıdır. PoW protokolü ile karşılaştırıldığında PoS protokolü büyük oranda enerji tasarrufu sağlamaktadır. Ama madencilik maliyeti neredeyse sıfır olduğu için ağa yapılacak saldırılara karşı daha savunmasız olabilmektedir. Birçok blokzinciri uygulaması başlangıçta PoW'u benimsemekte ve daha sonra PoS'a kademeli olarak dönüşüm sağlamaktadır. Örneğin, Bitcoin’ den sonra dünyanın en büyük sanal parası olan Etherum bir çeşit PoW olan Ethash'tan bir PoS türü protokol olan Casper'e geçmeyi planlamaktadır.

3. PBFT (Practical Byzantine Fault Tolerance) PBFT, Bizans Generalleri problemine benzer sorunlar için çözüm sunan bir protokoldür. Hyperledger Fabric uygulaması, uzlaşma protokolü olarak PBFT protokolünü kullanarak, yeni bir bloğun eklenmesi aşamasında 1/3 oranında kötü niyetli Bizans Generalleri tarzı saldırılarının üstesinden gelmektedir. Bu protokolde her bir değişiklik işlem öncesi, işlem ve işlem onayı olarak üç aşamaya ayrılır. Bir düğümün bir değişiklik yapabilmesi için ilgili değişiklik için her aşamada diğer düğümlerin 2/3’ ünden daha fazla onay alabilmesi gerekmektedir. PBFT benzer olarak, Stellar Consensus Protokolü (SCP) de Bizans Generalleri gibi problemlere çözüm sunan bir protokoldür. PBFT'de, her düğümün diğer düğümleri sorgulaması gerekirken SCP, katılımcı düğümlere hangi düğümlere inanılması gerektiğine dair öneri ve seçme hakkı verir.

4. DPOS (Delegated proof of stake) PoS protokolünde demokrasi uygulanırken, DPOS protokolünde ise temsili demokrasinin uygulanmaktadır. Ağdaki düğümler blok oluşturma ve doğrulama işlemleri için delegeler seçer ve blok doğrulama ve onaylama işlemleri az sayıda seçilmiş delege sayesinde çok hızlı yapılabilir. Bu arada, blok boyutu ve blok aralıkları gibi ağ parametreleri delegeler tarafından düzenlenebilir. Bitshares uygulaması, uzlaşma protokolü olarak DPOS kullanmaktadır.

5. Ripple Ripple, büyük bir ağda bulunan güvenilir alt ağların uzlaşmasına dayalı bir protokoldür. Ağdaki düğümler, uzlaşma süreçlerine katılımcı olan sunucu düğümler ve sadece varlık transferi yapan istemci düğümler olarak ikiye ayrılmaktadır. Zincirde bir işlemin onaylanması sırasında uzlaşmaya katılımcı düğümlerin uzlaşma oranlarına bakılır, bu oran % 80 ve üzerinde bir değere ulaşabilmişse işlem onaylanır ve tüm ağ için yayınlanır.



Tablo 2’de uzlaşma protokolleri ağa yeni bir düğüm eklenmesi, enerji tasarrufu, bir işlemin kabulü için gerekli onay oranı ve örnek uygulama kriterlerine göre karşılaştırılmıştır. PBFT protokolünde ağa yeni bir düğüm eklenmesi aşamasında ilgili düğümün bilgilerinin tanımlanması gerekmektedir. Diğer uzlaşma protokollerinde herhangi bir kısıtlama olmadan ağa yeni bir düğüm eklenebilmektedir. Enerji tasarrufu bakımından bir karşılaştırma yapılırsa, PoW protokolünde madenciler karmaşık bilgisayar hesaplamalarını çözmek için çok fazla elektrik ve bilgisayar gücü harcamaktadır. PoS ve DPOS protokollerinde madencilerin yaptıkları işlemler, çok daha az enerji ile tamamlanabilmektedir. PBFT ve Ripple protokollerinde madencilik yapılmamaktadır dolayısıyla diğer protokollerle karşılaştırıldığında büyük oranda enerji tasarrufu sağlanmaktadır. PoW protokollerinde ağın kontrol edilmesi için genellikle 51% oranında özet değeri çözümü gerekmektedir. Ama bencil madencilik stratejileri ile bu değer 25% oranlarına inebilmektedir. PBFT protokolünde bir düğümün kabul edilmesi için diğer düğümlerden 2/3 oranından onay alması gerekmektedir. Ripple protokolünde ise bu oran 80%’dir. Bu uzlaşma protokollerini kullanan uygulamalar için birer örnek vermek gerekirse, PoW için Bitcoin, PoS için Peercoin, PBFT için Hyperledger Fabric, DPOS için Bitshares, Ripple protokolü için ise Ripple uygulaması gösterilebilir. İyi bir uzlaşma protokolü verimli, kullanışlı ve güvenli olmalıdır. Son zamanlarda, blokzincirindeki uzlaşma protokollerini geliştirmek için bir dizi çalışma yapılmıştır. Bu çalışmalardan biri olan PeerCensus blok oluşturma ve onaylama işlemlerinin birbirinden ayırarak uzlaşma işlemlerini önemli ölçüde hızlandırmayı hedeflemiştir. Yüksek blok üretim oranları Bitcoin gibi PoW kullanılan uygulamaların güvenliğini riske atabilmektedir.

Kraft, bir bloğun sabit bir hızda üretilmesini sağlamak için GHOST adlı zincir seçim kuralını önermiştir. GHOST, en uzun zincir dalı yerine, dalların yüklerini dikkate alarak madenciler için daha verimli seçimler yapılmasını sağlayabilmektedir. Chepurnoy vd. ise madenciler için önceki blokların tüm verisi yerine sadece blok başlıklarının saklanmasına ilişkin bir çözüm sunmuştur.

**Blockchain network ve frameworkleri incelemeleri**

Dataların kayıt edilebilmesi için farklı farklı ihtiyaçlara hitap eden frameworkler ve network çeşitleri vardır. Bunlardan başlıcaları şunlardır: Cosmos-SDK Tendermint-BFT, Hedera Hashgraph, IOTA, Ethereum’dur.

**Tendermint BFT ve Cosmos SDK nedir**

(3)Yakın zamana kadar, bir blockchain oluşturmak, her üç katmanı da ( Networking , Consensus ve Application ) sıfırdan oluşturmayı gerektiriyordu. Ethereum, herkesin Akıllı Mantık şeklinde özel mantığı dağıtabileceği bir Sanal Makine blok zinciri sağlayarak merkezi olmayan uygulamaların geliştirilmesini basitleştirdi. Bununla birlikte, blok zincirlerinin gelişimini basitleştirmedi. Bitcoin gibi, Ethereum da çatallanması ve özelleştirilmesi zor olan yekpare bir teknoloji yığını olmaya devam ediyor. Bu, Jae Kwon tarafından 2014 yılında oluşturulan Tendermint'in devreye girdiği yer.

Tendermint BFT, bir blockchain'in ağ ve fikir birliği katmanlarını genel bir motora paketleyen ve geliştiricilerin karmaşık temel protokolün aksine uygulama geliştirmeye odaklanmalarını sağlayan bir çözümdür . Sonuç olarak, Tendermint yüzlerce saatlik geliştirme süresinden tasarruf sağlar. Tendermint'in ayrıca bizans hata toleranslı (BFT) adını da belirttiğini unutmayın.fikir birliği algoritması Tendermint BFT motorunda kullanılır. Fikir birliği protokolleri ve BFT tarihi hakkında daha fazla bilgi için Tendermint kurucu ortağı Ethan Buchman'ın bu harika podcast'ini kontrol edebilirsiniz . Tendermint BFT motoru denilen bir soket protokolü tarafından uygulamaya bağlı olan Başvuru Blockchain Arabirimi (ABCI). Bu protokol, herhangi bir programlama dilinde sarılabilir, bu da geliştiricilerin ihtiyaçlarına uygun bir dil seçmelerini mümkün kılar.

Ama hepsi bu kadar değil . Tendermint BFT'yi son teknoloji ürünü bir blockchain motoru yapan özellikler:

Herkese açık veya özel blockchain hazır: Tendermint BFT, bir blockchain için sadece ağ ve fikir birliğini işler , yani düğümlerin işlemleri ilerletmesine ve doğrulayıcıların blockchain'e eklemek için bir dizi işlem üzerinde anlaşmasına yardımcı olur. Bu rolü uygulama katmanı biçimini tanımlamak üzeredoğrulayıcı setioluşur. Geliştiriciler bu nedenle Tendermint BFT motorunun üzerine hem kamu hem de özel blok zincirleri inşa edebilirler . Uygulama, doğrulayıcıların söz konusu kaç jetona göre seçildiğini tanımlarsa, blockchain şu şekilde karakterize edilebilir:Bahis Kanıtı (PoS). Bununla birlikte, uygulama yalnızca sınırlı sayıda önceden yetkilendirilmiş varlıkların doğrulayıcı olabileceğini tanımlarsa, blockchain izin verilen veya özel olarak karakterize edilebilir. Geliştiriciler, blok zincirlerinin validator setinin nasıl değiştiğini tanımlayan kuralları özelleştirme özgürlüğüne sahiptir.

Yüksek Performans: Tendermint BFT, 1 saniyelik bir blok süresine sahip olabilir ve saniyede binlerce işleme kadar işlem yapabilir.

Anında kesinlik: Tendermint konsensüs algoritmasının bir özelliği anlık kesinliktir. Bu, onaylayıcıların üçte birinden fazlası dürüst (bizans) olduğu sürece çatalların asla oluşturulmadığı anlamına gelir. Kullanıcılar, bir blok oluşturulduğu anda işlemlerinin tamamlandığından emin olabilirler (Bitcoin ve Ethereum gibi İş Kanıtı blok zincirlerinde durum böyle değildir).

Güvenlik: Tendermint konsensüsü sadece hataya dayanıklı değildir, aynı zamanda sorumludur. Blockchain çatallanırsa, sorumluluğu belirlemenin bir yolu vardır .

Cosmos SDK ve diğer uygulama katmanı çerçeveleri

Tendermint BFT, bir blockchain'in geliştirme süresini yıllardan haftalara indirir, ancak sıfırdan güvenli bir ABCI uygulaması oluşturmak zor bir görevdir. Bu yüzdenCosmos SDK'sı bulunmaktadır.

Cosmos SDK Tendermint BFT üstünde güvenli blockchain uygulamaları oluşturmak işlemini basitleştiren bir genelleştirilmiş çerçevesidir. İki ana ilkeye dayanmaktadır:

Modülerlik: Cosmos SDK'nın amacı, bir ekosistem oluşturmaktır. Modüller geliştiricilerin kolayca dönmesini sağlar uygulamaya özel blok zincirler. Uygulamalarının her bir bitini sıfırdan kodlamak zorunda kalmadan. Herkes Cosmos SDK için bir modül oluşturabilir ve blockchain'inizde hazır modüller kullanmak bunları uygulamanıza aktarmak kadar basittir. Örneğin, Tendermint ekibi, aşağıdakiler için gerekli olan bir dizi temel modül inşa ediyor:Cosmos Merkezi. Bu modüller, kendi uygulamalarını oluştururken herhangi bir geliştirici tarafından kullanılabilir. Ayrıca, geliştiriciler uygulamalarını özelleştirmek için yeni modüller oluşturabilirler. Cosmos ağı geliştikçe, SDK modüllerinin ekosistemi genişleyecek ve karmaşık blockchain uygulamaları geliştirmeyi giderek daha kolay hale getirecektir.

Yeteneklere dayalı güvenlik: Yetenekler modüller arasındaki güvenlik sınırlarını kısıtlar, geliştiricilerin modüllerin bileşimi hakkında daha iyi bir neden yapmalarını ve kötü amaçlı veya beklenmedik etkileşimlerin kapsamını sınırlamalarını sağlar.

Cosmos SDK ayrıca komut satırı arabirimleri (CLI), REST sunucuları ve diğer yaygın olarak kullanılan çeşitli yardımcı program kitaplıkları oluşturmak için bir dizi yararlı geliştirici aracıyla birlikte gelir.

Son bir açıklama: Cosmos SDK, tüm Cosmos araçları gibi modüler olacak şekilde tasarlanmıştır. Bugün, geliştiricilerin Tendermint BFT üzerine inşa etmelerine izin veriyor. Bununla birlikte, ABCI'yi uygulayan diğer tüm konsensüs motorlarıyla kullanılabilir. Zaman geçtikçe, farklı mimari modellerle oluşturulmuş ve birden fazla konsensüs motoruyla uyumlu, hepsi tek bir ekosistem olan Cosmos Ağı'nda birden fazla SDK'nın ortaya çıkmasını bekliyoruz.

Cosmos-SDK default süreleri bir işlemin 6 saniyede onaylanmasına yöneliktir. Bu süre içerisinde bir account bir işlem gönderebilir diğerleri onaylanmaz. Bu süreyi config dosyalarında değiştirebilirsiniz.

Cosmos-SDK'sı ile Tendermint-BFT blockchain motorunu kendiniz inşa edebilir ve kendi sunucularınızda barındırabilirsiniz. İşlem başına ödenen gas miktarını kendiniz ayarlayabilirsiniz. Ve ödenecek gas miktarlarını kendi token cinsinizden kullanıcılarınıza ödetebilirsiniz.

Kullanıcılar isterlersede staking yaparak token kazanabilirler.

**Hedera Hashgraph**

(5) Merkezi olmayan uygulamalar

Kamuya açık defter kullanan uygulamalar ve mikro hizmetler her zamankinden daha fazla şeffaflık ve güven sağlar. Bu, sanatçılara doğrudan ödeme yapan bir müzik akışı hizmeti veya denetimler gerektirmeyen aralanmış bir reklam ağı gibi tamamen yeni şeyleri mümkün kılar. Hedera'da daha adil, daha güvenli, dijital bir gelecek dağıtılıyor.

Bitcoin merkezi olmayan altyapıya öncülük etti ve Ethereum programlanabilirlik getirdi. Ancak daha önceki iş kanıtı blok zincirleri, kabul edilebilir güvenlik seviyelerine ulaşmak için büyük miktarda enerji tüketir ve işlemleri yavaşça işler. Bu teknolojiler tarafından yoğun bant genişliği tüketimi, basit bir kripto para birimi işlemi için bile pahalı ücretlere yol açar.

Hashgraph konsensüsüyle güçlendirilen Hedera kazık kanıtı kamu ağı, yüksek hızlı işlem hızları ve inanılmaz derecede düşük bant genişliği tüketimi ile mümkün olan en yüksek seviyede güvenlik ( ABFT ) sağlar. Yüksek verimi, düşük ücretleri ve kesinliği saniyeler içinde birleştiren Hedera, kamu defterlerinin geleceğine yol açar.

**IOTA**

(4) IOTA’s Tangle is an open, feeless and scalable distributed ledger, designed to support frictionless data and value transfer.

Next Generation Data And Value Exchange

New Economies. New Possibilities.

IOTA is the first distributed ledger built for the “Internet of Everything” - a network for exchanging value and data between humans and machines.

Designed Entirely Without Fees.

No blocks. No Miners. When you send an IOTA transaction you validate two other transactions. This allows IOTA to overcome the cost and scalability limitations of blockchain.

IOTA Is The Backbone Of IoT

The IOTA network is built to for the Internet of Things, with tamper-proof data, feeless micro transactions and low resource requirements.

Enabling The Machine Economy

IOTA is posed to play a central role in the next industrial revolution, enabling economic relationships between machines and bridging the human and machine economies.

The Tangle

The Tangle is IOTA's network. It immutably records the exchange of data and value. It ensures that the information is trustworthy and cannot be tampered with nor destroyed.

Highly scalable

Increased network activity decreases transaction settlement times.

Low resource requirements

Designed for devices, such as sensors, to participate in a low-energy network.

Zero-fee transactions

Send 1 cent, receive 1 cent. Send $1,000,000, receive $1,000,000.

Fast transactions

IOTA transactions are confirmed within minutes.

Optional Quantum Robustness

With Winternitz signatures IOTA is resilient to the next generation of computing.

Decentralized

A globally distributed network, IOTA is resilient and robust against attacks.

**Ethereum**

(1)Ethereum networkünün hızı işlemin tamamlanma süresi, ne kadar gas ücreti belirttiğinize ve ağın sıkışıklığına göre değişmektedir.

Gönder'i tıkladığınızda, işleminiz bekleyen işlemler havuzuna girer. Oradan, Ethereum madencileri bekleyen işlemleri seçer ve bunları bir işlem bloğu halinde toplar .

Basitçe söylemek gerekirse, madencilik süreci, esasen bir matematik bulmacasını (çözülmesi zor ancak çözüldükten sonra doğrulanması kolay) çözmek için madenciler arasında bir rekabet içerir. Sorunu çözen ilk madenci, Ethereum blok zincirine bir işlem bloğu ekleyecek ve bloktaki işlemler tarafından ödenen tüm gazı içeren ödülü toplayacak.

Ortalama bir günde, standart gaz fiyatını öderseniz, bir işlemi işlemek 15 saniye ile 5 dakika arasında sürer .

Gazın fiyatını ne belirler?(10)

Açık artırmalar yapar. Bir bloğu, her koltuğun açık artırmada olduğu bir uçağa benzer gibi düşünebilirsiniz. Uçakta sadece çok fazla koltuk var, bu yüzden hedeflerine hızlı bir şekilde ulaşmak için motive olan insanlar oturduklarından emin olmak için daha fazla ödeme yapmayı düşünmezler. Diğerleri oraya ulaştıklarından korkmazlar; uçak bileti bütçe dahilinde kaldığı sürece bir sonraki uçuşa geçip geçmediklerini umursamıyorlar.

Ethereum'da benzer bir şey yaşayacaksınız. Sadece belirli sayıda işlem bir bloğa sığabilir. Madenciler ücretlerini en üst düzeye çıkarmak istiyorlar, bu yüzden bloklarına en yüksek gaz fiyatına sahip işlemleri dahil etme eğiliminde olacaklar. Bu nedenle, işleminizin sizin için ne kadar önemli olduğuna karar vermeli ve ardından buna göre ödeme yapmalısınız. Aceleniz varsa, ortalama bir kişiden daha fazlasını ödemek istersiniz; Aksi takdirde, gelecekteki bir bloğa çarpabilirsiniz. Çünkü ortalama gaz fiyatının altında ödeme yaparsanız, Ethereum işleminizin tamamlanması için ortalamanın üzerinde beklemeyi bekleyebilirsiniz.

Yavaş işlemlere ne sebep olur?

En basit cevap: ağ tıkanıklığı . Arz ve talep yasalarını düşünüyorsanız, bu tam mantıklıdır. Tartıştığımız gibi, arz - yani herhangi bir bloktaki alan - sınırlıdır. Ancak talep sınırlı değildir. Böylece, bir bloğa dahil edilen bir işlem alma talebi arttıkça, maliyet de (yani gaz maliyeti) artar. Genel olarak konuşursak, işlemlerini hızlı bir şekilde işlemek için ne kadar çok insan rekabet ederse, gaz fiyatını o kadar yükseltir.

Öte yandan, Ethereum işleminizin tamamlanması için acele etmiyorsanız, standart gaz fiyatından daha az ödeyerek bazı ETH'lerden tasarruf edebilirsiniz.

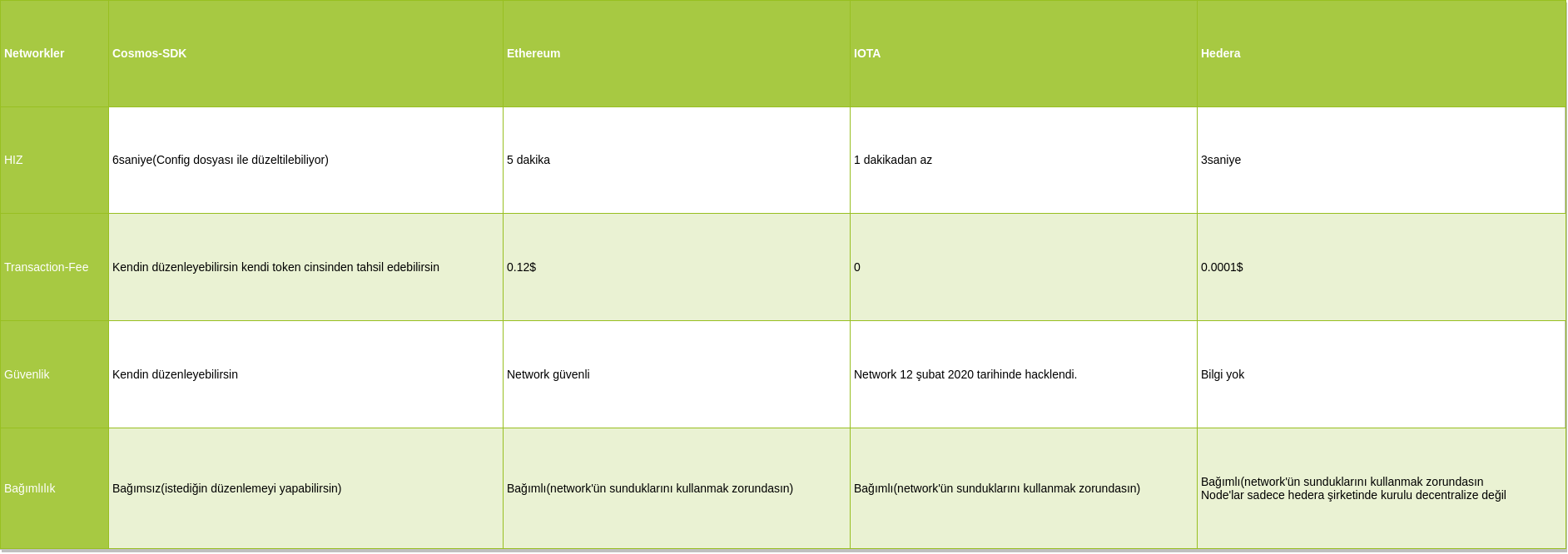
Yüksek gaz fiyatlarının yaygın nedenleri

Yüksek gaz fiyatlarının yaygın nedenlerinden biri kısa vadeli fiyat oynaklığıdır. Fiyatlar çok fazla arttığında, gaz fiyatlarının yükselme eğiliminde olduğunu fark etmiş olabilirsiniz. Bunu düşünmeniz mantıklıdır: fiyatlar yükseldiğinde veya boşaldığında, insanlar pozisyonlarını korumak veya arbitraj fırsatlarına atlamak ister. Bu genellikle fonların taşınmasını ve merkezi olmayan borsalar gibi akıllı sözleşmelerle etkileşime girilmesini gerektirir. Bu durumlarda, tüccarlar genellikle hedefledikleri kar fırsatlarını kaçırmamalarını sağlamak için daha yüksek ücretleri kabul ederler.

Yüksek gaz fiyatlarına yol açabilecek bir diğer durum bir airdrop’tur. Bu, bir uygulama veya oyunun belirteçlerini çok sayıda kullanıcıya, genellikle nispeten kısa bir sürede dağıtmaya çalıştığı zamandır.

Gas ücreti nedir? (2)

Bir işlemin yapılması ve ethereum nodelarına dağılması için ödenilen ücrete transaction fee denir. Transaction fee ise gas\_miktarıXgas\_ücreti çarpımından oluşmaktadır.



**Yüz tanıma sistemi nedir?**

(6) Yüz tanıma, Biyometri kişilerin fiziksel ve davranışsal özelliklerini göz önüne alarak yürütülen kimlik belirleme çalışmaları olarak tanımlanır. Bu kişi özelliklerine örnek olarak, retina ve iris görüntüleri, el geometrisi, Ayak izileri ve parmak izleri, elin damar görüntüsü, konuşma sesi, yüz özellikleri, kulak memesi, yürüyüş, klavye kullanım şekli, konuşma devinimleri örüntüleri verilebilir. Daha genel anlamda, biyometri bilişim teknolojilerinin bir parçası olup, insanların fiziksel özelliklerini ve davranış biçimlerini irdeleyip kişiyi tanıma amaçlı ipuçları çıkaran bir bilim dalıdır. Bizim içinde çalıştığımız bu biyometrik in içinde yüz özelliklerine bağlı insan tanıma, diğer bir deyiş ile “yüz bulma ve yüz tanıma”dır. Yüz tanımadaki üç temel unsur şöyle tanımlanır:

- Kişi tanılama: Bir nüfus dağarcığı içinde bir kişinin kim olduğunu anlamak.

- Kişi doğrulama: Belirli bir kimlik savıyla başvuran kişinin savının doğru olup olmadığını anlamak.

- Kişi onaylama: Kişinin önceden kayıtlı kişi olup olmadığını, kayıtlı ise bu kaydın güncellenmesini sağlamak.

Yüz Tanıma Sisteminin Ana Yapıtaşları

Tipik bir yüz tanıma sisteminin ana yapıtaşları şöyle sıralanır:

- Devşirilme ve kayıt: Kişiler, bir ya da birden fazla zZaman diliminde bir ya da daha fazla fiziksel/davranışsal özelliklerini ölçtürerek sisteme kayıt olurlar.

kamu defterl

- Veri işleme: Ölçülen yüz özellikleri süzgeçlenir, gürültüden arıtılmaya çalışılır, veriler istatistiksel olarak değerlendirilir, veri sınıflandırıcılar alıştırma döneminden geçirilir, birden fazla veri parçası veya karar mekanizması tümleştirilmeye çalışılır. Mesela, yüz imgelerini ele alalım. Yüz imgeleri, ısıl kamera, derinlik kamerası, ışık kamerası, stereo kamera veya video kamerası ile elde edilir. Ham veriler, poz kestirimi, ışıklandırma kaynaklı etkilerin giderimi, farklı ölçekteki yüzlerin aynı boya getirilmesi gibi önişlemlere tabi tutulur. Bu şekilde düzgelenmiş (normalized) yüzlerden öznitelik vektörleri çıkarılır, sadeleştirilir ve gürbüzleştirilir, sınıflandırıcılar eğitilir ve geçerlilik testleri tamamlanır. Bu aşamada her kişi bir yüz şablonu ile tanımlanmaktadır. Birden fazla veri gösterimi, birden fazla şablon ya da karar mekanizması kullanan sistemlerde tümleştirilmeden yararlanılır.

- Test: Bir terminalden oturum açmak isteyen ya da korumalı bir yerleşkeye girmeye çalışan bir kişinin o anki ölçümlerinden yola çıkılarak yeni bir şablonu oluşturulur ve bu test şablonu, şablon kütüphanesinde daha önce elde edilmiş şablonlarla karşılaştırılarak tanımaya çalışılır. Geçerli bir kişinin sistem tarafından tanınamayıp reddedilmesi oldukça olumsuz bir deneyim yaratacağından tanıma doğruluğunun yüksek olması gerekir. Öte yandan yanlış kabul olasılığı yüksekse yetkisiz kullanıcıların ve sahtekarların giriş yapması kolaylaşır. Bu bakımdan yüz tanıma sisteminin güvenilirliği, hem yanlış ret olasılığının düşük, hem de yanlış kabul olasılığının düşük olmasını gerektirir. Bu durum “Eşit Hata Oranı” diye tanimlanir.

Teknolojik olarak “Bağımsız Bileşenler Analizi, Asal Bileşenler Analizi ve Dinamik Yerel Farklandırıcı Analizi metotlarindan ortaya cikarilmis metotlardir.

**Güvenlik sistemi nedir?**

(7) Bir güvenlik alarmı yetkisiz girişi - - Bir bina veya diğer alana böyle bir ev veya okul gibi saldırı tespit için tasarlanmış bir sistemdir. Güvenlik alarmları, hırsızlık ( hırsızlık ) veya mülk hasarına karşı korunmanın yanı sıra davetsiz misafirlere karşı kişisel koruma için konut, ticari, endüstriyel ve askeri mülklerde kullanılır . Yerleşim bölgelerindeki güvenlik alarmları, hırsızlığın azalmasıyla bir korelasyon göstermektedir. Araba alarmları da araçların ve içeriklerinin korunmasına yardımcı olur. Hapishaneler ayrıca mahkumların kontrolü için güvenlik sistemleri kullanmaktadır .

Bazı alarm sistemleri hırsızlığa karşı tek bir amaca hizmet eder; kombinasyon sistemleri hem yangın hem de izinsiz giriş koruması sağlar. İzinsiz giriş alarm sistemleri , davetsiz misafirlerin faaliyetlerini otomatik olarak kaydetmek için kapalı devre televizyon gözetim (CCTV) sistemleriyle de birleştirilebilir ve elektrikli kilitli kapılar için erişim kontrol sistemlerine arayüz sağlayabilir . Sistemler, küçük, müstakil gürültü çıkarıcılardan bilgisayar izleme ve kontrolüne sahip karmaşık, çok taraflı sistemlere kadar uzanır. Panel ve İzleme istasyonu arasında iletişime izin veren iki yönlü ses bile içerebilir.

PROBLEM FORMULATION

Yüzün tespit edilmesinde ve blockchain’e kayıt edilmesinde kullanılması planlanılan yöntem:

1- Kamera bilgisayarında yüzün tespit edilmesinde kullanılan kütüphaneler real-time olarak ortam taraması yapacak şekilde açık bırakılır

2- Ortam taramasında tespit edilen yüzün faceID’si ilk olarak cache’e alınması ile başlanılır.

3- Kamera 10 saniye boyunca bir daha o kişinin yüzünü tespit etmezse o kişinin kamera tarafından ne kadar süre boyunca o ortamda kaldığı bilgisi ile beraber blockchaine kayıt işlemi gerçekleştirilmiş olur. Real-time olarak her frame’de faceID’sinin blockchaine kayıt edilmesi sistemin şişirmese neden olur. Bu çözüm ile sistemin şişmesinin önüne geçilmiş olur.

Bu kamera sisteminde tespit edilen kişilerin yüzlerin (dataların) kullanılması ise şu şekilde olmaktadır:

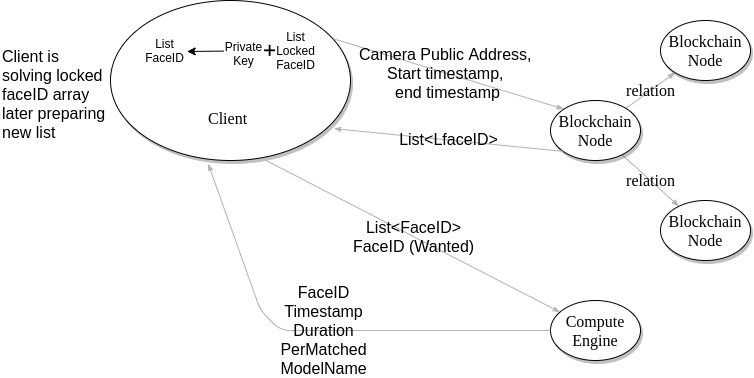
1- Aranılan kişinin faceID’si alınır.

2- Aranılmak istenilen zaman aralığı belirlenir

3- Blockchain sisteminde kayıt edilen datalardan o zaman aralığında tespit edilmiş olan kişilerin şifreli faceIDlerinin listesi alınır.

4- Blockchainden alınan faceID listesindeki tüm datalar şifreli olarak kayıt edildiği için şifreli dataların şifresi çözülmüş olarak yeni şifresiz olarak faceID listesi hazırlanmalıdır.

5- Compute Engine’e şifresiz faceID listesi ve aranılan kişinin faceID’si verilir ve eşleşme oranı sonuçlarına bakılır.



Compute Engine nedir?

Compute Engine: Bu terim sadece yüzlerin yüzde kaç oranında eşleşme olduğunu hesaplayan bilgisayarlara verdiğim isimdir. Blockchain sisteminin içerisine yapay zeka ile FaceID’lerinin karşılaştırılmasının yapılması blockchain nodelarını yoracağı için eşleştirmeler için Compute Node kullanılacaktır. Compute Node içerisine liste şeklinde o zaman dilimi arasında tespit edilen tüm faceID’ler verilir ve aranılan faceID verilerek Compute Engine’den o liste içerinde aranılan faceID ile eşleşen yüz olup olmadıgının tespiti istenilir. Sadece yüzlerin karşılaştırılmasını yapan içerisinde yapay zeka çalışan hesaplama nodudur.

Kaynakçalar:

1- [https://ethgasstation.info/blog/ethereum-transaction-how-long/#:~:text=On%20an%20average%20day%2C%20it,pay%20the%20standard%20gas%20price](https://ethgasstation.info/blog/ethereum-transaction-how-long/" \l ":~:text=On an average day%2C it,pay the standard gas price).

2- <https://ethereum.stackexchange.com/questions/19665/how-to-calculate-transaction-fee>

3- <https://cosmos.network/intro>

4- <https://www.iota.org/get-started/what-is-iota>

5- <https://www.hedera.com/>

6- [https://tr.wikipedia.org/wiki/Y%C3%BCz\_tan%C4%B1ma\_sistemi](https://tr.wikipedia.org/wiki/Yüz_tanıma_sistemi)

7- <https://en.wikipedia.org/wiki/Security_alarm>

8- <http://www.duzce.edu.tr/yonetim-bilisim-sistemleri/sayfa/10332/blockchain-nedir->

9- <https://www.researchgate.net/profile/Mustafa_Tanriverdi/publication/334816800_Blokzinciri_Teknolojisi_Nedir_Ne_Degildir_Alanyazin_Incelemesi/links/5d42860f299bf1995b5b892c/Blokzinciri-Teknolojisi-Nedir-Ne-Degildir-Alanyazin-Incelemesi.pdf>

10- https://ethereum.stackexchange.com/questions/19665/how-to-calculate-transaction-fee