Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-12

Kripto Para, Blokzincir Sistemi ve Siber Güvenlik İlişkisi

https://ugurozker.medium.com/10-soruda-blokzinciri-kripto-para-ve-borsalar-117c686e26c9

Siber Para

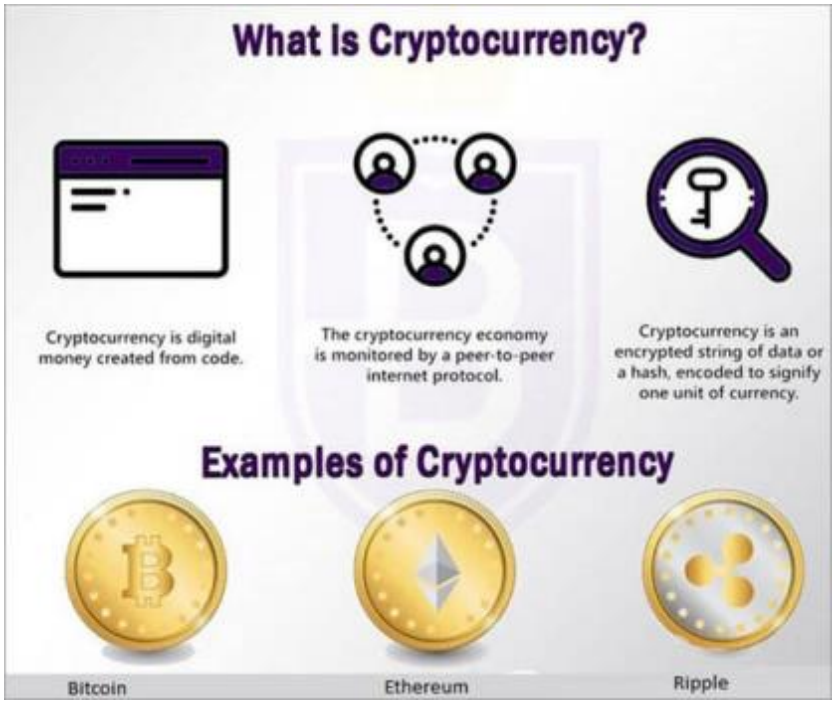
Dijital Para: Elektronik olarak saklanan ve transfer edilebilen paralardır. Elektronik ödemenin ilk örnekleri arasında, Hollanda'da gece yakıt alan kamyon şoförlerini ve benzin istasyonlarını hırsızlığa karşı korumak için tasarlanan akıllı kartlara para yükleyerek, bu paralarla yakıt alınabilmesi gösterilebilir.

Sanal Para: Herhangi bir merkez bankası, kredi kuruluşu veya e-para kuruluşu tarafından ihraç edilmediği halde, dijital paraya benzeyen ancak kağıt parayı temsil etmeyen sanal paralar ortaya çıkmıştır.

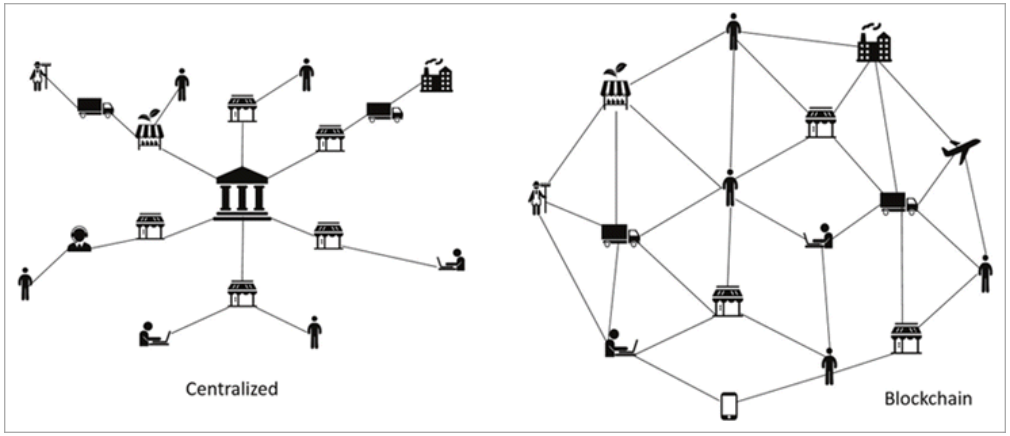
Kripto-Para: Son yıllarda kriptografik/şifreli oldukları için güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan kripto-paralar hem alternatif para birimi ve dijitaldirler hem de sanal paradırlar.

Siber Para

Bitcoin, elektronik ödemeler dahil olmak üzere sanal bir para biriminin kullanimini kolaylastiran çevrimiçi bir iletişim protokolüdür. İşlem leri herhangi bir tek sunucuda veya bir dizi sunucuda saklamak yerine, Bitcoin'e katilan bilgisayarlardan olusan bir ağa dagitilmis islemler üzerine kuruludur.



https://www.softwaretestinghelp.com/what-is-cryptocurrency/



https://www.softwaretestinghelp.com/what-is-cryptocurrency/

Kripto Para

Crypto ve currency kelimelerinin birlikte kullanılmasıyla ortaya çıkan cryptocurrency kelimesi kripto (şifreli) para manasına gelir.

Kripto paralar (cryptocurrency), eşler arası (Peer-to-Peer) mimaride birbirine bağlı madenci düğümü adı verilen bilgisayarlara ve blokzinciri yapısında tutulan kayıt sistemine dayanmaktadır. Bu sistemler sadece bir para birimi sağlamamakta, bu altyapılar üzerinde çeşitli 'merkezi olmayan' (decentralized), dağıtık (distributed) sistemler/yazılımlar tasarlanmaktadır.

İnternet üzerinde kullanılan, hiçbir merkezi otoriteye ya da aracı kuruma bağlı olmayan kripto para; bir tür sanal para birimini ifade eder. Kripto paralar sadece belirlenen şifrelerin kullanımıyla bulunduğu sanal cüzdanlardan, yine şifreler ile çıkarılıp kullanılabildiği için bu ismi taşırlar. Kripto para birimleriyle gerçek ya da tüzel kişiler, aynen piyasadaki nakit parayla yaptıkları gibi harcama ya da satış yapabilir.

Bitcoin

2008 yılında, takma ismi Satoshi Nakamoto olan bir programcı, Bitcoin adlı bir dağıtılmış katılımcılar arası dijital nakit tasarımını ortaya çıkarmıştır. Bitcoin Ocak 2009'dan değişim kuru bit başına 0,000764 $'lık bir fiyatla listelenene kadar (Ekim 2009), değersiz paraları çıkartan kriptografi meraklıları arasında zaman zaman belirsiz bir deneysel faaliyet olarak kalmıştır. 22 Mayıs 2010 tarihinde, Bitcoin'in ilk gerçek işleminde, bitcoin başına 0,0025 dolarlık bir değişim işlevi gördüğü kaydedilmiştir. O zamandan itibaren, bitcoin ile 160 milyondan fazla işlem gerçekleşmiş, satın alma gücü 2017'de bitcoin başına yaklaşık 900$ seviyesine yükselmiş ve toplam ticarete konu olan para arzı 150 milyar dolar civarında bir piyasa değerine ulaşmıştır [12].

Bitcoin'in temel tekniği olan blockchain 2009 yılında ilk çıkışından itibaren umut verici bir uygulama beklentisi oluşturmakta ve akademi ve iş dünyasında çok dikkat çekmektedir. İlk kripto para birimi olan Bitcoin, 2015 yılında en yüksek performans gösteren para birimi ve 2016 yılında en iyi performans gösteren emtia olarak değerlendirilmiş olup, Mayıs 2017 itibariyle günlük 300.000'den fazla onaylanmış işleme sahiptir [5].

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

- **Blokzinciri**: Blokzinciri, zamana göre sıralanmış ve sürekli büyüyen bir veri yapısıdır. Bloklar, yapılan işlem(ler)i ve bir önceki blokun adresini tutarlar. Blokzinciri, işlemlerin değiştirilemez listesinin tutulduğu bir kayıt defteridir (ledger). Ethereum'un kullandığı bloklarda çalıştırılabilir kod da bu blok içerisinde tutulmaktadır.

- **Akıllı Anlaşma (Smart Contract):** Ethereum projesi ile blokzincirinde akıllı anlaşmalar yapmak mümkündür. Bu anlaşmalarla; değer tutan, veri kaydeden ve çeşitli hesaplama görevleri için bloklara çalıştırabilir kod ekleyen uygulamaların geliştirilmesi mümkün olmaktadır.

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

- **Madenci Düğüm (Mining Node):** İşlemlerin gerçekleşmesini sağlayan bilgisayarlardır. Önceleri işlemci gücü kullanılırken, ekran kartlarındaki işlemcilerin veya bu iş için üretilmiş özel kartların kullanılması söz konusu olmuştur.

- **Madencilik Gücü:** Hash işlemleri çoğunlukla ekran kartlarının işlemcileri üzerinde GPU hesaplama gerçekleştirilmekte ve H/s (saniyede hash hesaplama) birimi ile Kilo-Mega-Giga (bin, milyon, milyar) biriminden güçleri tanımlanmaktadır. Bir ekran kartı Mh/s güçlerinde çalışmakta, makinelere takılan çoklu kartlarla yüksek madencilik güçlerine ulaşılabilmektedir

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

- **Konsensus Protokolleri:** Blokzincirlerinin bütün düğümlerde aynı olabilmesi için kimin değişiklik yapacağını belirleyen kurallar bütünüdür. PoW ve PoS yaklaşımlarından söz etmek mümkündür. Çalıştığının Kanıtı (**Proof of Work, PoW**), her düğümün değişiklik önerisi yapabilme hakkı kazanmak için öncelikle çözmesi gereken bir bulmaca gibidir. Başkalarının çözmesinin zor olduğu ama işleyen tarafından kolaylıkla doğrulanabilecek bir değerdir. **PoS** (**Proof of Stake**), PoW'deki hesaplama yerine, sisteminde sahip olduğu zenginliğe (kripto para) göre bloğu yaratacak olanın seçildiği bir yaklaşımdır.

- **Hesap:** Her makine veya kullanıcıya özgü o kripto para birimini tutmaya yarayan tekil (unique) bir hesaptır.
- Örneğin:

a94f5374fce5edbc8e2a8697c15331677e6ebf0b

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

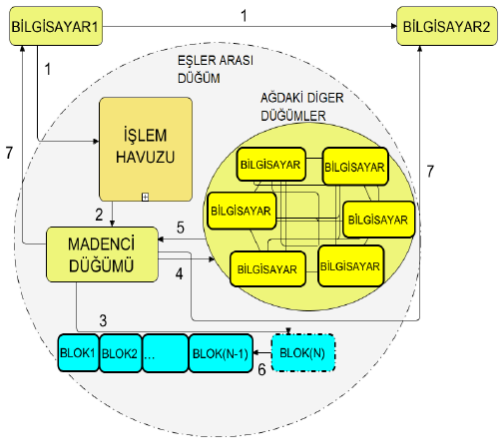
- Sistemin temel özellikleri:
  - İşlemler merkezi değildir,
  - İşlemler P2P ağda tüm düğümlere yayınlanır (broadcast),
  - İşlemler birden fazla düğüm tarafından onaylanır ve sonunda blokzincire eklenir,
  - Sistemdeki bütün hesaplar halka açıktır (public) ama anonimdir. Hesap ID'si aynı zamanda açık anahtar (public key) olarak kullanılır,
  - Madenci düğümler, işlemleri bloklar olarak toparlar.

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

- Blokzinciri uygulamasında madenci adı verilen sistemler, şu ana kadarki bütün işlemleri içeren bütün blokzincirini tutarlar. Bloğu oluşturacak düğümün seçimi konsensus protokolü ile gerçekleştirilir.

- Blokzinciri yapısı kullanan bir uygulama aracılığı ile Bilgisayar1 ve Bilgisayar2 makineleri arasında bir işlem yapılacağı bir senaryodaki yeni bloğun oluşturulması ve blokzincirine eklenmesi Şekil'de gösterilmiştir. İşlem aşamaları şekilde gösterilen numaralarla aşağıdaki gibidir:

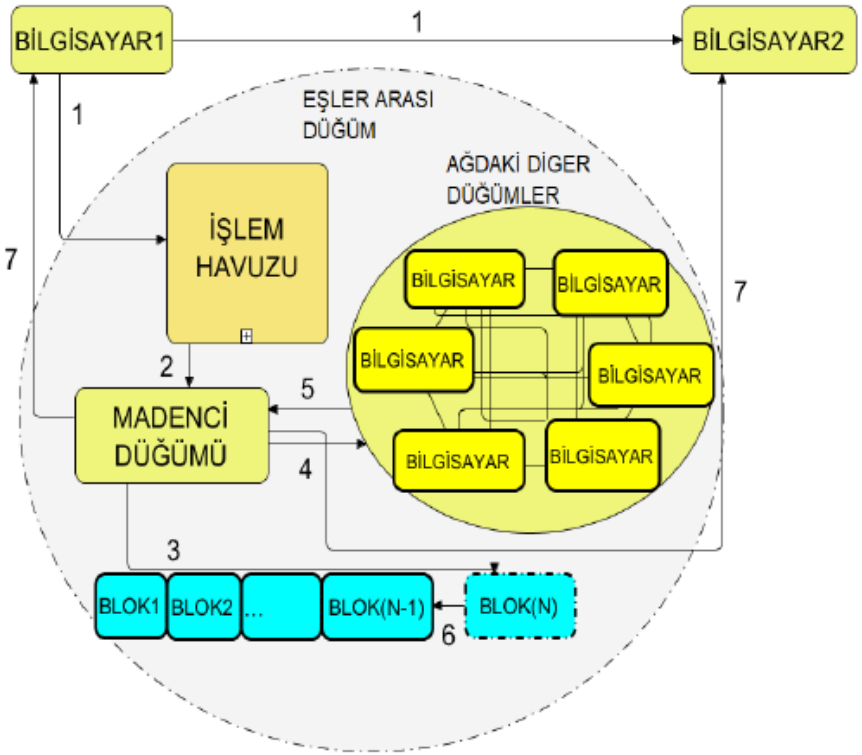


Blokzinciri tabanlı uygulamada yeni bloğun zincire eklenme süreci

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

1. Bilgisayar1 yapılacak işlemi Bilgisayar2 de dâhil olmak üzere eşler arası ağda yayınlar,
2. Sistemde işlem havuzunun (mining pool) kullanımı seçimli olabilmekte, işlemler yayınla öğrenilebilmektedir. Doğrulanmamış işlemler, düğümler tarafından çağırılır,
3. Ağda kullanılan protokole göre, n adet işlem toplu olarak bir bloğa yazılabilir. Düğümler tarafından yeni blok oluşturulur,
4. Doğrulama için eşler arası ağdaki bilgisayarlara yayın yapılır,
5. Doğrulama bilgisinin tamamlandığı bilgisi ağ içerisinde iletilir,
6. Eşler arası ağda konsensus protokolü ile bir madenci düğümü seçilir. Seçilen madenci düğümü, yeni bloğu blokzincirine ekler,
7. Talep edilen işlemin tamamlandığı bilgisi, işlemi gerçekleştiren makinelere iletilir.

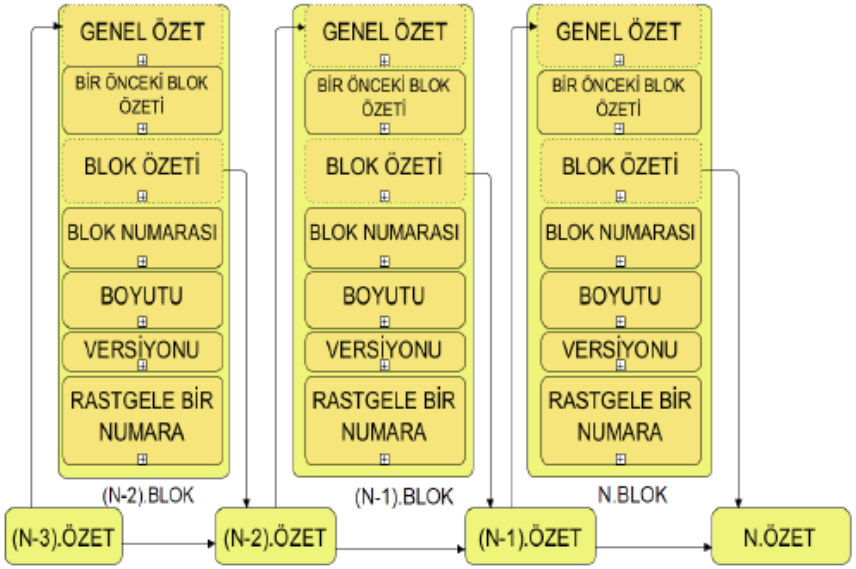


Blokzinciri tabanlı uygulamada yeni bloğun zincire eklenme süreci

https://dergipark.org.tr/tr/download/article-file/516266

SİSTEMİN GÜVENİLİRLİĞİ (RELIABILITY OF THE SYSTEM)

Saldırganların sistemi ele geçirmesi için, ağdaki düğümlerin çoğunluğunu ele geçirmesi gerekmektedir. Düğümlerin dağıtık olması, bu olasılığı da oldukça düşürmektedir.

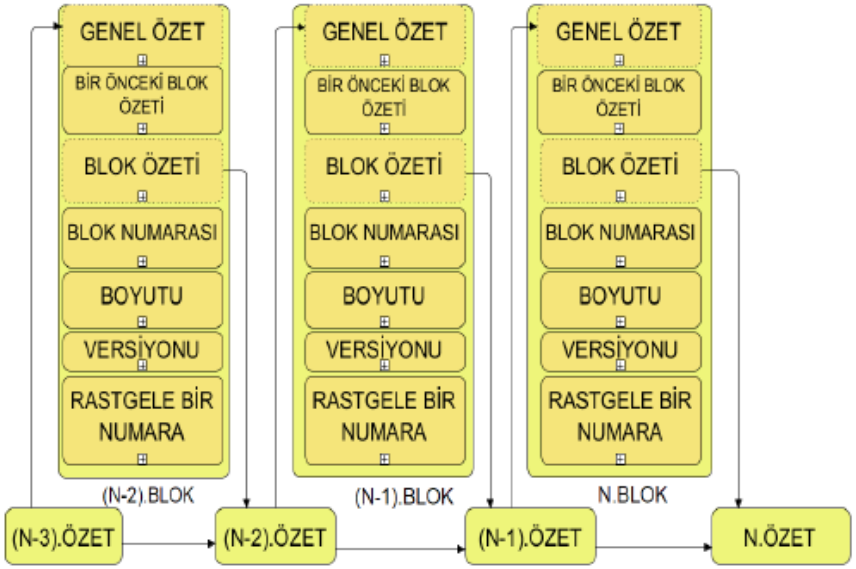


Şekil 2. Blokzinciri yapısı

Blokzinciri yapısında hash fonksiyonları aktif olarak kullanılmaktadır. Her blok, bir önceki bloğun sağlamasını (hash) tutar. Hash fonksiyonu olarak farklı algoritmalar da kullanılmakla birlikte, BTC SHA256 algoritmasını kullanmaktadır. Sistemdeki bir işlemi değiştirmek, zincirdeki tüm blokları da hesaplamayı gerektirecektir ki bu da muazzam bir işlem gücüne gereksinim duyacaktır.

https://dergipark.org.tr/tr/download/article-file/516266

SİSTEMİN GÜVENİLİRLİĞİ (RELIABILITY OF THE SYSTEM)



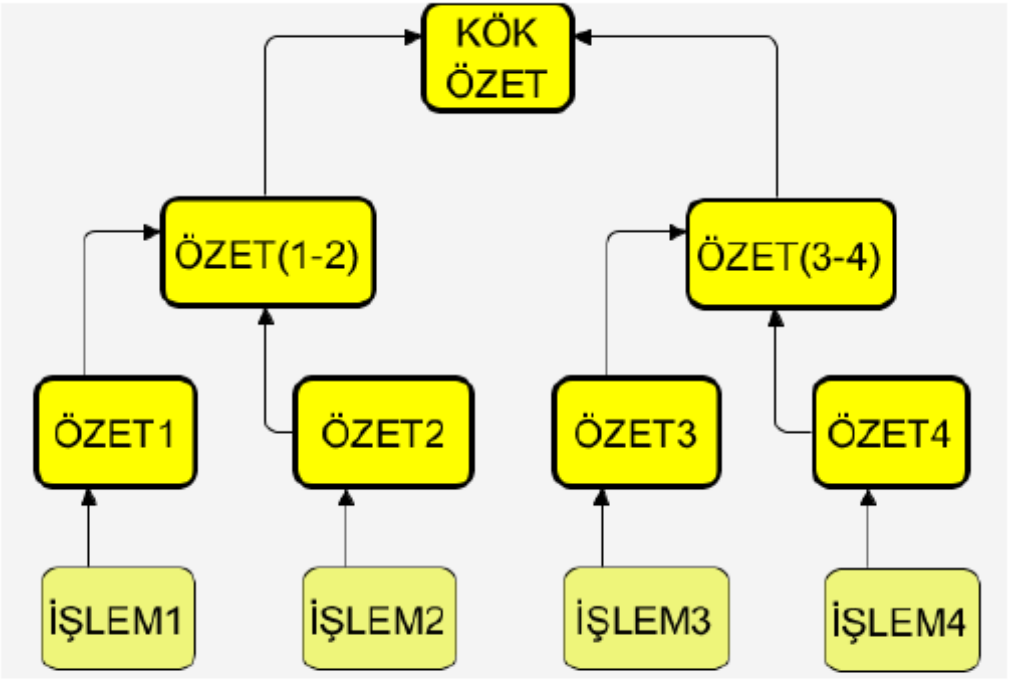
Şekil 2. Blokzinciri yapısı

Zincirdeki her değiştireceği blok için diğer düğümleri de ikna etmesi ve bunun için de PoW hesaplamalarını gerçekleştirebilmesi gerekecektir. Bu da %51 saldırısı olarak tanımlanmaktadır, çünkü bunun için ağdaki bütün düğümlerin madencilik işlemci gücünün en az %51'ine sahip olması gerekecektir. Saldırı teorik olarak mümkün olsa da pratikte bu tür bir saldırı olası değildir ve etkisinin kısa süreceği ifade edilmektedir. PoS kullanıldığında ise, saldırganın bütün kripto paranın en az %51'ine sahip olması gerekecektir ki Ethereum'da sadece konsorsiyumun elinde bulunan bir güçtür.

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

Bloklar, hash (özet) değeri ile önceki bloklara bağlanmaktadır. Bu süreçte önceki bloklardaki özet değerinden genel özet değeri oluşturulmaktadır. Aynı zamanda bir önceki bloğun özeti de tutulmaktadır. Blok içerisinde ise; 4 işlemin toplanarak bir bloğa yazılması durumunda alınan özetlerden kök özet (Merkle ağacının) oluşturulması Şekil'de gösterilmiştir.



Şekil 3. Merkle ağacının oluşturulması

https://dergipark.org.tr/tr/download/article-file/516266

Blokzinciri Nasıl Çalışır (How Blockchain Works)

Şekil 6. Blokzincirin çalışması [34]
(Working schema of blockchain)

Blokzincirinde içerisinde veri bulunduran her işlemin zincire eklenmesi sonucu zincirin boyutu giderek artmaktadır. İşlemlerin boyutu belirli bir büyüklüğe eriştikten sonra yeni bir blok oluşturulmakta ve bir önceki blok ile ilişkilendirilerek zincire eklenmektedir.

https://dergipark.org.tr/tr/download/article-file/775807

Blokzinciri Nasıl Çalışır (How Blockchain Works)

Şekil 6. Blokzincirin çalışması [34]
(Working schema of blockchain)

Bir işlem kaydının doğrulanması ve zincire eklenmesi süreci şekil'deki gibi gerçekleşmektedir. Şekilde blokzincirin nasıl çalıştığının daha iyi anlaşılması için örnek bir senaryo oluşturulmuştur. Örneğin A kişisi B kişisine bir miktar sanal para ya da dijital bir karşılığı olan başka bir varlık göndermek istemektedir. Sanal paralar bir adres tarafından tanımlanan dijital bir cüzdanda saklanmaktadır. A kişisi aktarım işlemi için aktarmak istediği sanal para miktarını ve B kişisine ait dijital cüzdanın adresini belirler ve bu bilgiler A kişisinin cüzdanına ait gizli anahtar ile şifrelenir. Böylece bu işlemin A kişisi tarafından oluşturulduğu anlaşılır ve ağdaki başka biri tarafından değiştirilmesi engellenmiş olur.

https://dergipark.org.tr/tr/download/article-file/775807

Blokzinciri Nasıl Çalışır (How Blockchain Works)

Şekil 6. Blokzincirin çalışması [34]
(Working schema of blockchain)

Şifrelenen işlem daha sonra yayınlanmak üzere ağa gönderilir. Diğer ağ düğümleri dijital imzayı analiz ederek bu işlemin A kişisine ait olup olmadığını kontrol ederler. Daha sonra A kişisinin cüzdanındaki bakiyenin B kişisine göndermek istediği tutarı karşılayıp karşılayamayacağı bilgisi, karşılıyorsa da A kişisinin aynı zaman aralığında başka kişilere de para transferi yapıp yapmadığı yani olası bir çift harcama durumunun tespit edilmesi gerekmektedir. Bu kontroller dışında karşılaşılan uyuşmazlıkların çözülmesi ve güvenlik ihlallerine karşı bir korumanın oluşturulması da gerekmektedir.

https://dergipark.org.tr/tr/download/article-file/775807

Blokzinciri Nasıl Çalışır (How Blockchain Works)

Şekil 6. Blokzincirin çalışması [34]
(Working schema of blockchain)

Blokzincirinin tutarlılığı ve güvenliği için bahsedilen bu kontrollerin ve korumanın sağlanması çok önemlidir. Blokzincirinde merkezi bir yapı bulunmadığı için ağdaki düğümler tarafından uyulması gereken kurallar belirlenmeli ve bir uzlaşma mekanizması oluşturulmalıdır. Ağdaki düğümlerin uzlaşması sonrasında ilgili işlem yeni bir bloğa eklenir, yeni blok belirli bir boyuta ulaştıktan sonra önceki bloklar ile bağlantılı olarak zincire eklenir. Yeni bloğun zincire eklenmesi ve yayınlanması sonrasında, işlemde yer alan tutar B kişisinin cüzdanına eklenecek ve A kişisinin cüzdanından düşülecektir. Yapılan bu işlemin kaydı şeffaf olarak izlenebilecek ve ağdaki tüm düğümlerde kayıtlı olacağından dolayı değiştirilmesi veya silinmesi mümkün olmayacaktır.

https://dergipark.org.tr/tr/download/article-file/775807

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

Literatürde (Alanyazında) kullanılan blokzincir sistemleri

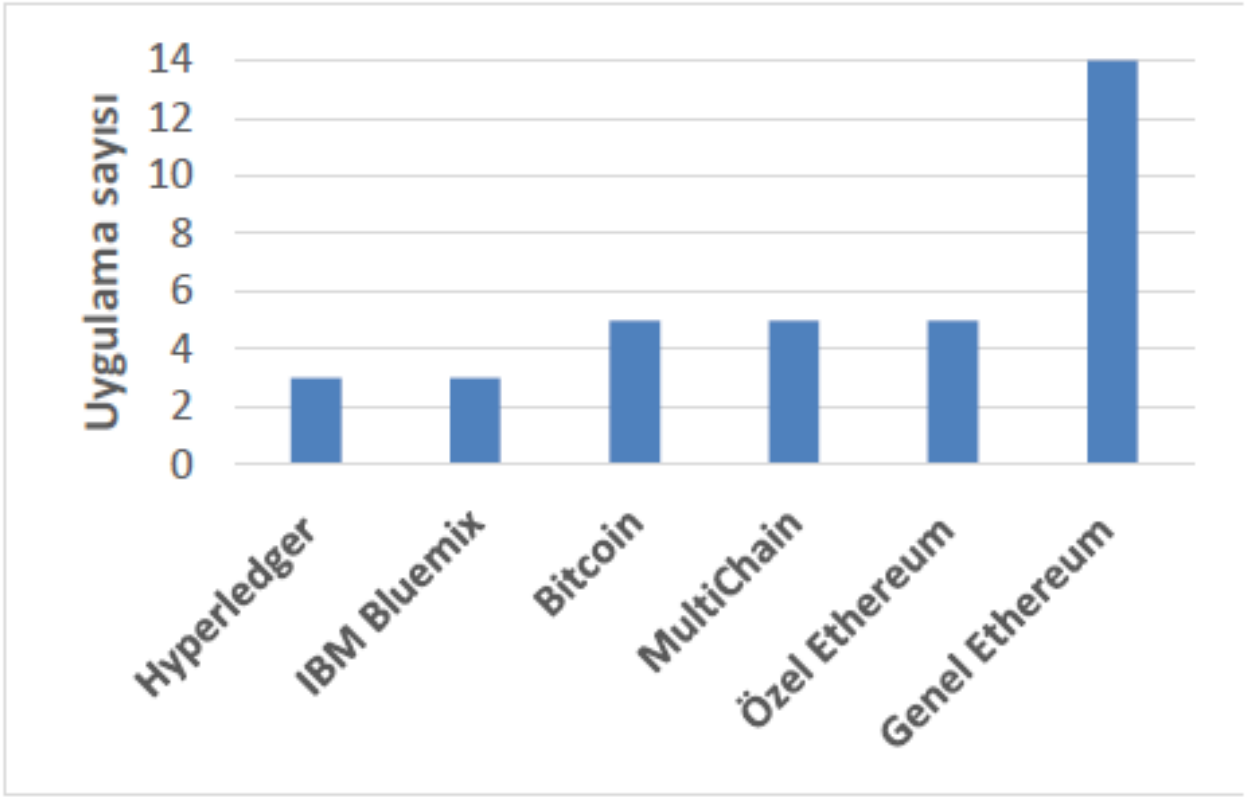
Blokzinciri tabanlı uygulamaların geliştirilmesi için çeşitli altyapı çalışmaları bulunmaktadır. Linux Foundation tarafından yürütülen Hyperledger, 27 organizasyonun destek verdiği bir açık kaynak projesidir.

Bunun yanı sıra farklı kripto paraları altyapıları da çeşitli API'ler sağlamaktadır. Örneğin; Ethereum blokzinciri platformu, akıllı anlaşmalar ile altyapıları üzerinde çeşitli uygulamaların çalıştırılmasına izin vermektedir.

Solidity gibi yüksek düzeyli dillerle Ethereum Sanal Makinesi (Ethereum Virtual Machine) üzerinde akıllı anlaşmalar geliştirmek mümkündür.

https://dergipark.org.tr/tr/download/article-file/516266

BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)



Şekil 3. Literatürde kullanılan blokzinciri sistemleri [32]
(*Blockchain systems used in literature*)

https://dergipark.org.tr/tr/download/article-file/775807

Blokzincir Teknolojileri

Blokzincir, merkezi bir sunucunun veya güvenilir bir otoritenin kaldırılmasına olanak sağlayarak, merkezi güvenin internet ortamında dağıtılmasına denir.

Blokzincir teknolojisi yaygın olarak Bitcoin ve Ethereum gibi sanal paraların altındaki teknoloji olarak bilinmektedir. Fakat bu teknoloji sağladığı olanaklar ve çeşitlendirilebilir uygulamaları ile çok daha geniş bir yelpazeye sahiptir.

Blokzincir teknolojisi, günümüzün önemli problemlerinden olan, tek merkeze dayalı güven sistemlerindeki merkezi güven yapısını dağıtarak, bu sistemlerin daha verimli çalışmasında oynayabileceği rol nedeniyle dikkat çekici hale gelmiştir. Blokzincir, veri transferi sağlayan mevcut internet ortamında, değerli varlıkların transferine de olanak sağlayarak tüm hayatımızı yeniden şekillendirecek yepyeni bir teknolojiyi adlandıran merkezi olmayan bir şifreleme kayıt defteridir.

https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincir Teknolojileri

Blokzincir modeli iki temel kavramdan meydana gelir: Blok zinciri oluşturan bloklar ve bu blokları oluşturan kayıtlar.

• **Kayıtlar:** Blokzincir kayıtları, ilgili blokzincir yapısının üzerine oluşturulduğu her türlü içerik bilgisidir. Bu bilgiler tasarıma göre para aktarımı, demirbaş girdisi, müşteri kayıtları gibi değerler olabilir. Sanal para birimleri için bu kayıtlar para transferi bilgileridir. Sistemde kayıtlı olan bir kullanıcıdan bir başka kayıtlı kullanıcıya yapılmış olan transferler bu kayıtlar ile tutulur. Yeni transfer istekleri de sıraya konularak bir sonraki işlem sırasında kaydedilerek yerini alır.

• **Bloklar:** Kayıtlar birleştirilip belirli aralıklarla işlenerek blokların içine yazılır. Blokların içerisinde kaç tane kayıt bulunacağı ve kayıtların hangi işlemlerden geçtikten sonra bir blok tevellüd edeceği gibi kıstaslar, blokzincirin tasarımına mahsustur. Genel itibariyle, bir bloğun oluşturulması sırasında kriptografik özet algoritmaları ve dijital imza kullanılır.

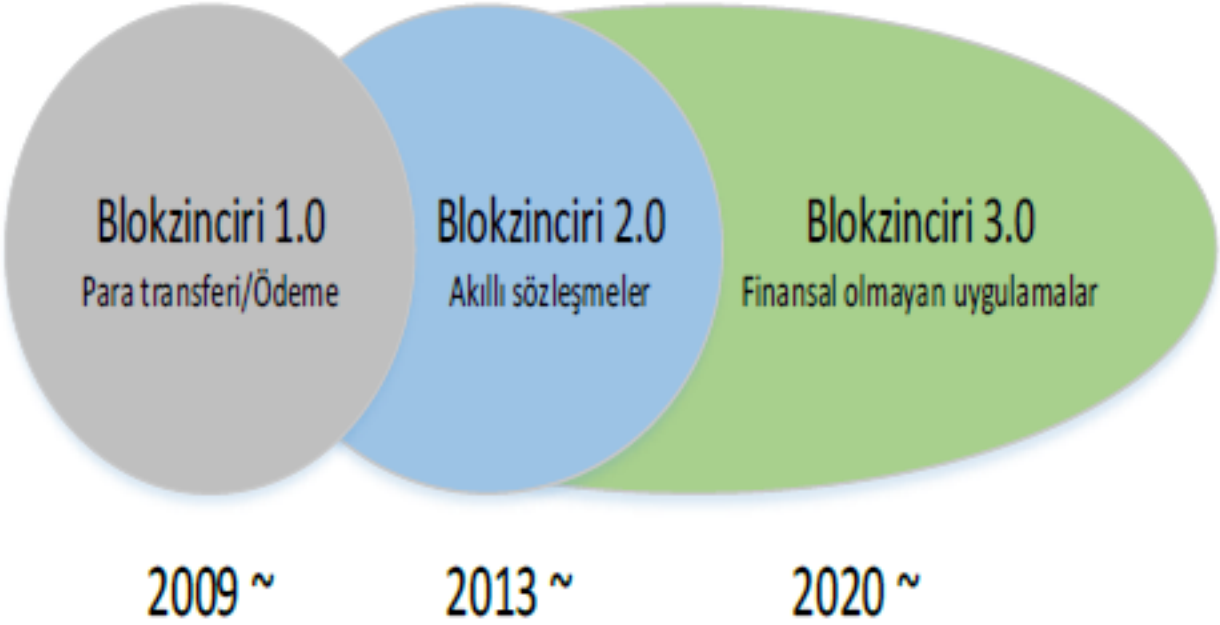
https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincir Teknolojileri

Blokzincir teknolojisinde her bir katılımcı, başlangıçtan itibaren tüm kayıtların bir kopyasını tutar. Bu kayıtların değiştirilmesi özetlerin değişmesine yol açacağından ötürü kayıtlar değiştirildiğinde çoğunluk bunu fark edebilir. Bu yüzden güvenilir ortamda merkezi bir veritabanı ihtiyacı ortadan kalkar. Herkesin doğrulama yapabildiği dağıtık bir veritabanı sistemi ile kimseye güvenmeye gerek kalmadan doğru bilginin tutulduğu ispatlanabilir.

https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincir Teknolojilerinin Geilişimi



Şekil 1. Blokzincirin Gelişimi [19]
(Evolution of blockchain)

https://dergipark.org.tr/tr/download/article-file/775807

Blokzincir Teknolojilerinin Geilişimi

Blokzinciri 1.0:

Dijital para evresi olarak da adlandırılan Blokzinciri 1.0, para transferi ve dijital ödeme gibi uygulamaları bulunan kripto paraları ifade etmektedir. Kripto paralarda madencilik, şifreleme ve blok yapısı gibi blokzinciri teknolojileri kullanılmaktadır. İlk kripto para olan Bitcoin uygulama olarak kuramın önüne geçmiştir. Bitcoin, para transferi ve elektronik alışverişler için geleneksel yöntemlerle kıyaslandığında çok küçük miktarlarda işlem ücreti gerektirmektedir. Bitcoin hesapları takma isimli olması sayesinde kredi kartlarına oranla daha fazla gizlilik sağlamaktadır. Geleneksel para birimleri, mali düzenlemeler ve para basma gibi işlemler için bir merkez bankasına bağlıdırlar bunun aksine, Bitcoin ve diğer dijital para birimleri ise sabit para arzını garantilemek için kriptografiyi kullanmaktadır. Bu sayede dijital paralar enflasyona karşı korunmaktadır.

https://dergipark.org.tr/tr/download/article-file/775807

Blokzincir Teknolojilerinin Geilişimi

Blokzinciri 2.0:

Dijital ekonomi olarak da ifade edilen Blokzinciri 2.0, basit ödemeler ve para transferi işlemlerin ötesinde çok çeşitli ekonomik ve finansal uygulamaları kapsamaktadır. Bu tür uygulamalar arasında, krediler ve ipotekler gibi geleneksel bankacılık araçları, hisse senetleri, tahviller, vadeli işlemler ve sözleşme gibi araçlar yer almaktadır. Bu tür kurallara bağlı karmaşık işlemler için akıllı sözleşmeler (smart contracts) kullanılmaktadır. Akıllı sözleşmeler blokzinciri ağı üzerinde bulunan belirli kurallara sahip bilgisayar programları olarak ifade edilebilir. Akıllı sözleşmeler, kullanımı son zamanlarda hızla yaygınlaşan bir blokzinciri teknolojisidir.

https://dergipark.org.tr/tr/download/article-file/775807

Blokzincir Teknolojilerinin Geilişimi

Blokzinciri 3.0:

Dijital toplum olarak da adlandırılan Blokzinciri 3.0, para, sözleşme, finansal uygulamalar dışında bilim, sanat, sağlık, eğitim, iletişim, yönetim ve denetim alanlarını da kapsamaktadır. Blokzinciri teknolojisinin gelecek vadeden en önemli uygulamalarından biri, akıllı yönetim, akıllı ulaşım, akıllı yaşam, doğal kaynakların akıllı kullanımı ve akıllı ekonomi gibi kavramların tümünü içeren akıllı kentlerdir. Nesnelerin interneti (internet of things) kapsamında makinelerin haberleşmesi (machine to machine) alanlarında blokzinciri teknolojisinden faydalanmak mümkündür. Dijital kimlik, bankacılık, siber güvenlik ve elektronik tıbbi kayıt sistemlerinde de blokzinciri teknolojilerinin kullanılması Blokzinciri 3.0 kapsamında değerlendirilebilir…

https://dergipark.org.tr/tr/download/article-file/775807

Blokzincir Teknolojisinin Geleceği

Bitcoin altyapısını oluşturan blokzincir teknolojisi gelecek vadeden bir teknoloji olmakla beraber bu teknolojinin tam bir olgunluğa erişmesi için kat edilmesi gereken adımlar vardır. Ancak, İsviçre merkezli Credit Suisse tarafından hazırlanan geniş çaplı bir rapora göre, blokzincir sadece dijital para birimleri veya finansal hizmetler için değil birçok alanda kullanılmaktadır. Dünya Ekonomik Forumu tarafından yapılan bir ankete göre, yöneticilerin %58'i küresel Gayri Safi Milli Üretimin %10'unu "2025'den önce blokzincirde bulunacak" şekilde bir tahmin yürütmektedir. Bu yıl rapora göre olgunluğa erişim yılı olarak belirtilmiştir. Şu anda bu teknoloji prototip ve deney aşamalarının arasında yer almaktadır.

https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincir Teknolojisinin Geleceği

Blokzincirin genel olarak uygulama alanları

- Bankacılık
- FinTech
- Para Transferleri
- Değerli Belgelerin Yaratılması ve Saklanması
- E-Ticaret ve Ödemeler
- Hisse Senetleri ve Borsalar
- E-Noter
- Kişiden Kişiye Borçlanma ve Dağıtık Yapılı Kredi Sistemleri
- Bağış Sistemleri ve Mikro Ödemeler
- Bulut Bilişim ve Güvenli Bulut Depolama

https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincir Teknolojisi

Blokzincirinin avantajları

- Verilerin bir kopyası tüm paydaşlar tarafından kaydedilir, herkes bu verilere erişebilir ve yapılan işlemleri görebilir. Verilerin bu şekilde saklanması sayesinde veri kaybı ve veri tahribatı önlenir.
- Dijital imza ve doğrulamalar sayesinde aracılara ihtiyaç duymadan paydaşlarını birbirine güvenmesini sağlanır.
- Herkes hem kendi işleminin durumunu hem de blokzincirindeki tüm işlemlerin ayrıntılarını görebilir, bu şekilde şeffaflık sağlanmış olur.
- Blokzinciri üzerindeki veriler değiştirilemez veya silinemez.
- Merkezi bir otorite olmadan çalışabilir, bu dağıtık yapısı sayesinde kontrol edilemez, iptal edilemez veya kapatılamaz.
- Akıllı sözleşmeler sayesinde belirli faaliyetler otomatikleştirilebilir.

https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincir Teknolojisi

Blokzincirin dezavantajları;

- Uzlaşma protokolü olarak proof of work (işin ispatı) kullanılan blokzincirlerinde çok fazla enerji tüketilmekte ve çok pahalı bilgisayar sistemleri çalıştırılmaktadır.
- Blokzincirindeki tüm veriler her bir düğümde ayrı ayrı saklanmaktadır ve her bir işlem sonrası bu düğümlerdeki verilerin tutarlılığı sağlanmaktadır. Örneğin zincire bir blok eklemek Bitcoin zincirinde 10- 60 dakika Ethereum zincirinde ise 15 saniye zaman almaktadır. Bu nedenle geleneksel veritabanları ile performans bakımından kıyaslandığında yetersiz kalmaktadır.
- Ağdaki her bir düğümün tüm verilerin bir kopyasını saklayabilmesi ve içeriğine erişebilmesi, kullanıcıların mahremiyetine zarar verebilir.
- Akıllı sözleşmeler bir kez oluşturulduktan sonra değiştirilemez ve blokzincirinde herkesin erişimine açık halde saklanır. Bu da akıllı sözleşmeleri kötü niyetli saldırılara karşı savunmasız bırakabilir.

https://avys.omu.edu.tr/storage/app/public/ybulut/131648/6-%20blokzincir.pptx

Blokzincirin siber güvenlik için kullanımı

- Yeni teknolojiler beraberinde yeni güvenlik tehditlerini getirmektedir. IoT, akıllı şehirler gibi popüler kavramların sağladığı yararların yanı sıra bilgi güvenliği konusunun iyi bir şekilde gözden geçirilmesi gerekmektedir.

- P2P tabanlı ve dağıtık blokzinciri mimarisi ile siber güvenlik için mahremiyet ve bütünlük başta olmak üzere çeşitli güvenlik servisleri sağlayacak çözümler yapmak mümkündür.

- Blokzinciri, kriptografik algoritmalar, dijital imzalar ve özet fonksiyonları gibi güvenlik yöntemlerini kullanmaktadır.

- Bankacılık sektörü, finans kuruluşları, sağlık hizmetleri, elektronik oylama, IoT ve bilgisayar ağları için kullanımı söz konusudur. Güvenlik ve mahremiyet alanı üzerine yapılan çalışmalarda blokzinciri tabanlı yaklaşımların kullanımı gelecek vaat etmektedir

https://dergipark.org.tr/tr/download/article-file/516266

Blokzincirin siber güvenlik için kullanımı

- Blokzinciri teknolojisinin bütünlük (integrity), anonimlik (anonymity) ve uyarlanabilirlik (adaptability) özelliklerini etkileyen unsurlar içermesi ve blokzinciri teknolojisinin veri depolama yönetimi, malların ve verilerin ticareti, kimlik denetimi ve değerlendirme sistemleri gibi kategorilerde kullanılması söz konusudur.
- IoT cihazlarının yönetimi için blokzinciri teknolojisinin kullanımı önerilmektedir. Platform olarak Ethereum'un seçildiği bu çalışmada, Ethereum'un akıllı anlaşması kullanılarak IoT cihazlarının davranışlarını belirleyen kodlar yazılmaktadır. Kimlik doğrulama amaçlı (authentication) kullanılan açık anahtarlı altyapı (Public Key Infrastructure, PKI) ile saldırganların Ethereum platformu üzerinde bulunan yönetim sistemini kontrol altına almasının önüne geçilmektedir. Anahtarların yönetimi için RSA kripto sistemi kullanılmaktadır. Açık anahtarlar (public keys) Ethereum'da, gizli anahtarlar (private keys) uçlardaki IoT cihazlarda saklanmaktadır.

https://dergipark.org.tr/tr/download/article-file/516266

Blokzincirin siber güvenlik için kullanımı

- Cihazlar arasındaki iletişimin ve hassas verilerin korunması ve IoT güvenliği ve mahremiyet için blokzinciri yaklaşımı önerilmektedir.
- Akıllı şehirlerdeki güvenlik tehditlerine karşı koruma sağlamak ve akıllı şehirleri daha güvenli bir hale getirmek için blokzinciri teknolojisinin kullanımı ele alınmıştır. Akıllı şehirlerde bulunan cihazlarla blokzinciri teknolojisinin entegrasyonunun dağıtık bir ortamda güvenli veri iletişimini sağlaması söz konusudur.
- Kişisel verilerin korunması ve mahremiyet amacıyla da blokzincirinin kullanımı mümkündür. Bilindiği üzere, üçüncü parti yazılımları veya servisleri çok fazla miktarda kişisel ve hassas verileri toplamaktadır. Blokzinciri tabanlı ve blokzinciri tabanlı olmayan depolama alanlarının birleştirildiği mahremiyet odaklı bir kişisel veri yönetimi platformu oluşturulması mümkündür.

https://dergipark.org.tr/tr/download/article-file/516266

Blokzincirin siber güvenlik için kullanımı

- Kişisel sağlık verilerinin tutulduğu elektronik sağlık kayıtlarına erişim denetim altında tutulmalıdır
- MedRec adını verdikleri blokzinciri çözümü tabanlı kayıt yönetim sistem: Hastaların, geniş kapsamlı ve değiştirilemez bir sağlık kaydına sahip olması ve bu kayda farklı sağlık kurumlarından kolaylıkla erişebilmesi hedeflenmiştir. Sistem, araştırmacı ve sağlık otoriterilerinin madenci olarak sisteme katkıda bulunması için anonim verileri bir ödül olarak vermeyi öngörmektedir. Madenci makineleri PoW ile sistemin güvenilirliğini sağlayacaktır.

https://dergipark.org.tr/tr/download/article-file/516266

Blokzincirin siber güvenlik için kullanımı

- Bilgisayar ağları için kullanımına dair bazı çalışmalardan da söz etmek mümkündür. Gelecekte blokzinciri tabanlı DNS ve blokzinciri tabanlı internet söz konusu olabilecektir. DNSChain [17]; özgür, güvenli ve dağıtık bir DNS çözümü olarak ortaya atılmıştır. SecureChain [18], ağ cihazlarının yapılandırma dosyalarının ve log kayıtlarının saklanmasına yönelik bir yaklaşımdır. Log kayıtlarının daha güvenli bir mimaride tutulması; değiştirilemezlik ve inkâr edilemezlik ilkesinin sağlanması hedeflenmektedir.

https://dergipark.org.tr/tr/download/article-file/516266

Blokzincirin siber güvenlik için kullanımı

- Blokzinciri teknolojisi işlemsel olarak maliyetlidir ve yüksek bant genişliğine gereksinim duyulmaktadır.
- Bu gereksinimler birçok IoT cihazı için uygun değildir. IoT'de blokzinciri teknolojisinin uygulanması; yüksek enerji tüketimi, ölçeklenebilirlik ve işleme zamanı gibi nedenlerden çok kolay değildir.
- IoT için iyileştirilmiş yeni bir blokzinciri mimarisi önerilmiştir literatürde. Bu çalışmada, Bitcoin'in altyapısını oluşturan klasik blokzinciri kullanımının getirdiği yükleri ortadan kaldırmak için hafif (lightweight) bir blokzinciri mimarisi kullanımını mümkündür.

https://dergipark.org.tr/tr/download/article-file/516266

Blokzincirin siber güvenlik için kullanımı

- Önerilen çözüm, merkezi konumda ve özel olan değiştirilemez bir kayıt defterinden (Immutable Ledger, IL) ve merkezi olmayan konumda ve herkese açık (public) blokzincirinden oluşan hiyerarşik bir mimariye sahiptir. IL, ek yükü azaltmak için IoT'nin yerel ağ seviyesinde çalışmaktadır. Blokzinciri ise daha güçlü bir güven için daha üst seviyedeki uç cihazlarda bulunmaktadır. IoT için iyileştirilmiş bu blokzinciri mimarisi, güvenlik ve mahremiyet özelliklerini içinde barındırmakta olup blok onayı işleme zamanını azaltmak için PoW yerine dağıtık güven yöntemini kullanmaktadır. Madencilik süreci yoktur, bu da bazı gecikmeleri ortadan kaldırmaktadır. Simülasyon sonuçları, önerilen yöntemin düşük oranda paket ve işlem yükü getirdiğini göstermektedir. Servis reddi saldırısı (Denial of Service, DoS), modifikasyon saldırısı (modification attack), düşürme saldırısı (dropping attack) ve ekleme saldırısı (appending attack) gibi bazı saldırı türlerine karşı da yöntemin başarısı ölçülmüştür

https://dergipark.org.tr/tr/download/article-file/516266

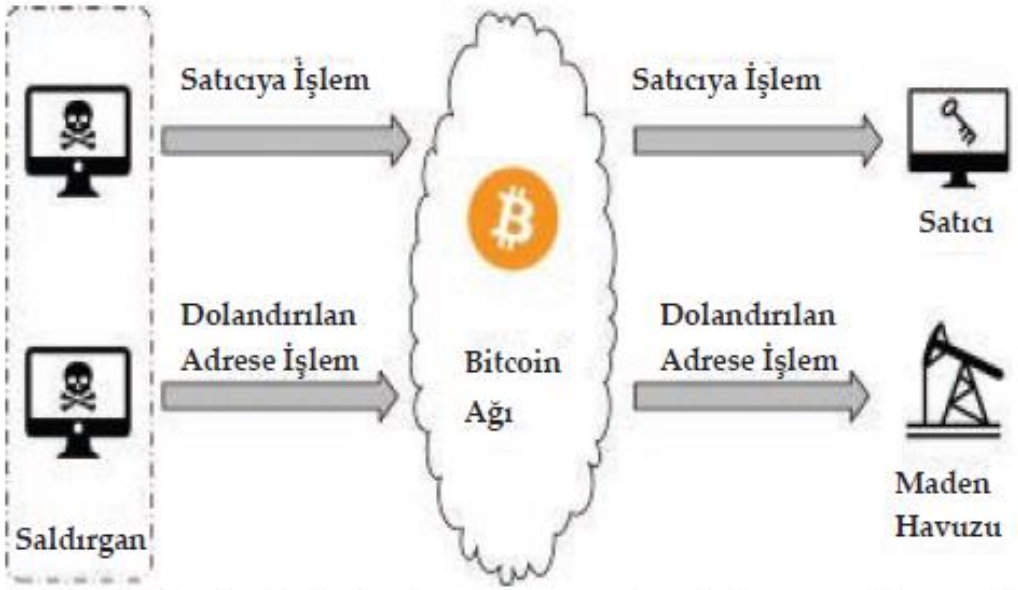
%51 Güvenlik Açığı

Blokzincir teknolojisinin karşılıklı güven tesis etmek için kullandığı dağıtık uzlaşma mekanizması %51 güvenlik zafi yetini de beraberinde getirmektedir. Tüm blokzinciri kontrol altına alabilmek için, uzlaşma mekanizmasının doğurduğu bu güvenlik açığı kötü niyetli kişiler tarafından kullanılabilir. Örneğin, en popüler iki kripto paranın kullandığı (Bitcoin ve Ethereum) işin kanıtı tabanlı blok zincirinde bu durum şu şekilde ortaya çıkabilir: Eğer tek bir madencinin özetleme gücü, tüm blok zincirinin toplam özetleme gücünün %50'sinden daha fazlasına tekabül ediyorsa, %51 saldırısı başlatılabilir. 2012 yılının ocak ayında, "ghash.io" isimli madencilik havuzu bitcoin hesaplama gücünün %42'sine ulaşmıştır. Bu olaydan sonra, bir dizi madenci gönüllü olarak havuzdan ayrılmıştır [15]. Öte yandan, diğer kripto paraların kullanmış olduğu diğer blokzincir teknolojilerinde, bu saldırının ortaya çıkma durumu teknolojiye bağlı olarak farklılık göstermektedir [3]

Blokzincir Sistemlerindeki Saldırı Tipleri

Çifte Harcama

Çift harcama, bir kullanıcının işlemler için aynı kripto parayı çok kez kullanmasıdır. Normalde, blokzincir teknolojisinin konsensüs özelliği işlemleri doğrulayabilmektedir. Buna rağmen, çift harcamanın önüne geçmek mümkün değildir.



Şekil 10.6. Bitcoin'deki hızlı ödemeye karşı yapılan çift harcama saldırı modeli

Bu durumu şu şekilde açıklayabiliriz: İşin kanıtı tabanlı blokzincirde, iki işlemin başlangıç ve doğrulama aşamaları arasında geçen süreyi saldırgan kendi çıkarı için kullanabilir. Yani, bu süre içerisinde bir saldırı başlatabilir. İlk işlemin çıktısı elde edilip, aynı kripto para ikinci işlem geçersiz sayılmadan önce tekrar kullanılırsa bu durum çift harcamaya tekabül etmektedir. Aslında, burada yapılan bir saldırıdır.

Blokzincir Sistemlerindeki Saldırı Tipleri

Sybil Saldırısı

Sybil saldırısı saldırganların mevcut düğümlerle anlaşarak kontrol sağlamak yerine sistemde çok sayıda kimlik ve düğüm oluşturarak faaliyet göstermelerini ve bu sayede kontrolü ele geçirmeye çalışmalarını ifade eder. Çoklu kimlik oluşturma yoluyla gerçekleşecek saldırılara karşı PoW mekanizmaları dayanıklıdır çünkü önemli olan sistemde kaç adet aktörün olduğu değil sistemdeki işlemci gücünün ne kadarının kontrol edildiğidir

Blokzincir Sistemlerine Yapılmış Saldırı Örnekleri

DAO Saldırısı

Bir kitle fonlama şirketi olan DAO, 28 Mayıs 2016 tarihinde Ethereum'da konuşlandırılmış bir zeki sözleşmedir. DAO, blokzincirde konuşlandırıldıktan sadece 20 gün sonra bir saldırıya uğramıştır ve saldırgan bu saldırısında zeki sözleşmenin yeniden giriş zafi yetini kullanmıştır. Saldırgan, geri dönme fonksiyonunda DAO'ya withdraw() fonksiyon çağrısı içeren kötü niyetli bir zeki sözleşme geliştirmiş ve bunu yayınlamıştır. Saldırının hemen öncesinde DAO'nun değeri 150 milyon dolar seviyesine kadar çıkmıştır. Kötü niyetli kişi/kişiler gerçekleştirdikleri saldırı sonucunda yaklaşık olarak 60 milyon dolar çalmışlardır.

Blokzincir Sistemlerine Yapılmış Saldırı Örnekleri

BGP Ele Geçirme Saldırısı

Sınır Geçiş Protokolü (BGP) standart bir yönlendirme protokolüdür ve IP paketlerinin hedefl erine nasıl yönlendirildiğini düzenler.

Kötü niyetli kişiler blok zincirinin ağ trafi ğini durdurmak için BGP yönlendirme protokolünü kullanmaktadırlar. Yalnız, BGP ele geçirme saldırısının gerçekleştirilebilmesi, ağ operatörlerinin kontrolünün ele geçirilmesine bağlıdır. Maalesef, bazı Bitcoin madencilik havuzları merkezi bir yapıya sahiptir. Saldırganlar bu tarz madencilik havuzlarına BGP ele geçirme saldırısı gerçekleştirirlerse, Bitcoin ağını bölebilirler veya blok yayılma hızını yavaşlatabilirler.

Gerçekleştirilen bir saldırıda, saldırganlar kendileri tarafından kontrol edilen bir maden havuzuna trafi ği yönlendirmişler ve yaklaşık olarak 83.000 ABD doları tutarındaki kripto para birimini iki aylık bir süre zarfında kurbanlarından toplamışlardır

Kripto Para Borsalarına Saldırı Örnekleri

- Bancor
- Bithumb
- Coinrail
- BitGrail
- Coincheck

Kripto Para Borsalarına Saldırı Örnekleri

Bancor

Bancor Temmuz 2018'de, tanımlanamayan aktörlerin akıllı sözleşmeleri yükseltmek için kullanılan bir cüzdanı tehlikeye att ığını itiraf etmiştir. İddiaya göre aktörler, 12.5 milyon ABD Doları 24.984 ETH ve 229.356.645 NPXS (Pundi X, yaklaşık 1 milyon ABD Doları) geri çektiler. Saldırganlar ayrıca Bancor'un yaklaşık 10 milyon dolarlık 3.200.000 BNT'sini de çaldılar. Bancor, planladığı uzlaşma ve güvenlik önlemlerinin ayrıntıları hakkında yorum yapmamıştır.

Kripto Para Borsalarına Saldırı Örnekleri

Bithumb

Saldırganlar Haziran 2018'de, saldırganlar Güney Kore'nin en büyük kripto para birimi borsası Bithumb'tan 30 milyon dolar değerinde kripto para birimi çalmışlardır. Cointelegraph Japan'a göre saldırganlar Bithumb'ın sıcak (çevrimiçi) cüzdanını kaçırmışlardır.

Kripto Para Borsalarına Saldırı Örnekleri

Coinrail

Coinrail, Haziran 2018'de, sisteminde "siber saldırı" olduğunu ve tahminen 40 milyar won (37.2 milyon $ değerinde) çalındığını itiraf etmiştir. Polis saldırıyı soruşturmaktadır, ancak daha fazla ayrıntı yayınlanmamıştır.

Kripto Para Borsalarına Saldırı Örnekleri

BitGrail

BitGrail Şubat 2018'de, müşterilerin Nano'daki (XRB)
195 milyon ABD Doları değerindeki kripto para biriminin çalındığını
iddia etmiştir.

Kripto Para Borsalarına Saldırı Örnekleri

Coincheck

Ocak 2018'de, tanımlanamayan saldırganlar borsadaki sıcak cüzdandan 523 milyon NEM para (yaklaşık 534 milyon USD) çalmışlardır. Coincheck, NEM'in daha güvenli bir çoklu imzalı cüzdan yerine tek imzalı sıcak cüzdanda tutulduğunu ve çalınan paranın Coincheck müşterilerine ait olduğunu doğrulamıştır.

Sorular

Bir sonraki ders Hukuki Açıdan Bilişim Suçları, Siber Güvenlik, Adli Bilişim Ve Güncel Teknolojiler konusuna giriş yapılacak.