Co-funded by
the European Union

ÜNİTE 2

Blockchain Kullanırken Güvenlik Stratejileri

EMC SERVICES

Co-funded by
the European Union

Blockchain Teknolojisinin Temelleri ve Önemini Anlamak

Bu blog yazısını AB tarafından finanse edilen “V2B: Sanat Mesleki Eğitim Kursiyerleri için Metaverse’de NFT Fırsatları Yaratmak” projesi için oluşturduk. Ve proje referans numaramız 2022-1-DE02-KA210-VET-000 080828. L4Y Learning for Youth GmbH tarafından Adana Çukurova Güzel Sanatlar Lisesi ve EMC Services Ltd. işbirliğiyle koordine edilen “Blockchain Teknolojisinin Temelleri ‘ni ve Önemini Anlamak” giriş yazısındaki eğitim çerçevesiyle ilgili olarak hazırlanmıştır.

Blockchain Teknolojisinin Temelleri modülü, blockchain teknolojisini kapsamlı bir şekilde anlamayı hedefler. Bu modül, teknolojinin temel kavramlarını ve önemini vurgular. Blockchain, verilerin depolanma, paylaşılma ve güvence altına alınma şekillerini yenileyen yıkıcı bir teknolojidir. Bu eğitim, blok zincirine yeni başlayanlar için genel özellikleri ve işlemleri hakkında temel bilgileri sunar. Ayrıca R2 kategorimizde daha fazla blog yazısı bulabilirsiniz. Bu yayınlardan biridir.

Blockchain Teknolojisinin Temelleri: Öğrenme Hedefleri

Bu modülün sonunda, öğreniciler aşağıdakileri yapmaya uygun olacaklardır:

- Blockchain teknolojisini ve başlangıçtaki genel özelliklerini tanımlayabilecektir.
- Blockchain ağının armatürünü ve faktörlerini açıklayabilecektir.
- Blockchain sistemlerinde güvenliğin ve güvenilirliğin önemini anlayabilecektir.
- Renkli işlemleri tanımlayabilecek ve blok zinciri teknolojisini uygulayabilecektir.
- Blockchainin uygulanmasıyla ilgili olası faydaları ve zorlukları tahmin edebilecektir.

Blockchain Teknolojisine Giriş

Bu bölümde, Blockchain Teknolojisinin Temellerini keşfedeceğiz. Bu teknolojiye dair temel bilgileri sağlayarak, blockchain dünyasının yeniliklerini anlamanızı hedefliyoruz. Yenilikçi bu teknolojinin gizemlerini adım adım çözeceğiz. Yalnızca güvenli işlemleri korumakla kalmayıp aynı zamanda güven kavramında devrim yaratan ve aracılara olan ihtiyacı ortadan kaldıran bir dijital defter hayal edin. Blok zincirinin doğuşu, dünyayı güvenli, sınırsız, eşler arası bir elektronik nakit sistemiyle tanıştıran Bitcoin blok zincirinin doğuşuyla 2009 yılına kadar uzanabilir. Bu bölüm, açık ve kapsayıcı kamusal blok zincirlerinden kontrollü özel veya izinli blok zincirlerine kadar çeşitli blok zinciri biçimlerini açıklamaktadır. Geleneksel iş modellerini yeniden şekillendirmeye ve yeni bir reform ve şeffaflık çağının önünü açmaya hazır olan blok zincirinin sınırsız potansiyelini keşfederken bize katılın.

Co-funded by
the European Union

Blockchain'i Tanıyalım

Blockchain, özünde, dijital bir defterin omurgası ve aracılara ihtiyaç duymadan güvenli varlık transferlerinin güvenilir bir koruyucusu gibidir. Bunu, tıpkı internetin dijital bilgi akışını kolaylaştırdığı gibi, dijital değer alışverişini kolaylaştıran bir teknoloji harikası olarak düşünün. Para birimlerinden mülk tapularına ve hatta oylara kadar, neredeyse değerli her şey tokenlara dönüştürülebilir, güvenli bir şekilde saklanabilir ve blok zinciri ağı içinde takas edilebilir.

Blockchain'in Doğuşu

Blockchain teknolojisinin doğuşu, Bitcoin blok zincirinin ortaya çıkışıyla birlikte 2009 yılına kadar uzanmaktadır. Bitcoin, sınırları aşan, güvenli, sansüre dayanıklı, eşler arası elektronik nakit sistemi kavramına öncülük etmiştir. Bitcoin herkese açık olduğu için, katılımın sınır tanımadığı açık veya izne tabi olmayan bir blok zincirinin en iyi örneğidir.

Blockchain'in Çeşitli Formları

Günümüz dünyasında Blockchain teknolojisinin temelleri, farklı ihtiyaçlara cevap vermek üzere çeşitli biçimler almıştır. Bazı Blockchainler belirli bir grup katılımcı için tasarlanmıştır ve erişimleri dikkatle kontrol edilir. Bunlara özel ya da izinli blok zincirleri diyoruz ve daha kontrollü bir ortam sunuyorlar.

Değer Transferinin Ötesi

Blockchain teknolojisi, güvenli değer transferlerini mümkün kılma rolünün ötesinde, büyüleyici bir özellik sunar. İşlemlerin silinmez bir izini yaratarak tekil bir gerçeklik oluşturur. Bu gerçek zamanlı şeffaflık, tüm katılımcılara fayda sağlayarak olayların kusursuz bir kaydının tutulmasını sağlar.

Bir Dönüşüm Dünyası

Kullanılan Blockchain protokolünün türüne bakılmaksızın, blok zinciri teknolojisi asırlık iş modellerini yeniden şekillendirmek için muazzam bir potansiyel barındırmaktadır. Devletlerin meşruiyetinin artmasının önünü açar. Ayrıca refah için yeni umutların kilidini kaldırarak faydalarını tüm vatandaşlara yayar.

Blockchain teknolojisinin büyüleyici dünyasına dalıyoruz. Dijital çağda etkileşim ve işlem yapma şeklimizde devrim yaratma gücünü keşfediyoruz. Bu yolculukta emniyet kemerinizi bağlayın.

Blockchain Teknolojisinin Temelleri: Blockchain Mimarisi ve Bileşenleri

Bu bölümde, bir Blockchain in yapısını inceleyeceğiz. Öğreniciler, halka açık, özel ve enstitü Blockchainleri dahil olmak üzere farklı Blockchain türlerini keşfedecekler. Darbeler, madenciler ve ambarlar da dahil olmak üzere bir Blockchainağının yapısına ilişkin algı kazanacaklar. Akıllı sözleşmelerle ilgili kısmı ve bunların Blockchain de tonlu sözleşmelerin yürütülmesini nasıl sağladığını anlayacaklar.

Blockchain nasıl çalışır?

Ana Blockchain mimarisi bileşenleri şunlardır:

Düğüm – Blockchain içindeki kullanıcı veya bilgisayar

İşlem – bir Blockchain sisteminin en küçük yapı taşı

Blok – ağdaki tüm düğümlere dağıtılan bir dizi işlemi tutmak için kullanılan bir veri yapısı

Zincir – belirli bir sıradaki bloklar dizisi

Madenciler – blok doğrulama işlemini gerçekleştiren belirli düğümler

Mutabakat- Blockchain işlemlerini yürütmek için bir dizi kural ve düzenleme

Blockchainin beş unsuru vardır: dağıtım, şifreleme, değişmezlik, tokenizasyon ve merkezsizleştirme.

Dağıtım:

Blockchain katılımcıları fiziksel olarak birbirlerinden ayrı konumdadır ve bir ağa bağlıdır. Her katılımcı tam bir düğüm işleterek, yeni işlemler gerçekleştikçe güncellenen bir defterin eksiksiz bir kopyasını tutar.

Şifreleme:

Blockchain, bloklardaki verileri güvenli ve yarı anonim olarak kaydetmek için açık ve özel anahtarlar gibi teknolojileri kullanır (katılımcıların hesapları / profilleri vardır). Katılımcılar kimliklerini ve diğer kişisel bilgilerini kontrol edebilir ve bir işlemde yalnızca ihtiyaç duydukları kadarını paylaşabilirler.

Değişmezlik:

Tamamlanan işlemler kriptografik olarak imzalanır, zaman damgası vurulur ve sırayla deftere eklenir. Katılımcılar gerekliliği konusunda anlaşmadıkça kayıtlar bozulamaz veya başka bir şekilde değiştirilemez.

Tokenleştirme:

Bir Blockchain zincirindeki işlemler ve diğer etkileşimler, güvenli değer değişimini içerir. Jetonlar şeklinde ortaya çıkan bu değer, finansal varlıklardan verilere ve fiziksel varlıklara kadar her şeyi temsil edebilir. Jetonlar aynı zamanda katılımcıların kişisel verilerini kontrol etmelerine olanak tanır ve bu da blok zincirinin iş durumunun temel bir faktörüdür.

Merkeziyetsizlik:

Hem ağ bilgileri hem de ağın işleyişine ilişkin kurallar, bir mutabakat mekanizması sayesinde dağıtılmış ağdaki düğümler tarafından korunurlar. Başka bir deyişle, merkeziyetsizlik, tek bir varlığın tüm bilgisayarları, bilgileri kontrol etmediği veya kuralları belirleyemediği anlamına gelir.

Kaynak: http://gartner.com/en

Blockchain Teknolojisinin Temelleri: Blockchain Güvenliği ve Güvenilirliği

Bu bölüm Blockchainlerin güvenlik ve güven bileşenlerine odaklanmaktadır. Dijital imzalar ve hash fonksiyonları gibi, blok zincirinde veri bütünlüğünü ve gerçekliğini korumak için hayati önem taşıyan kriptografik yöntemler incelenmektedir. Bu bölümde ayrıca Blockchain ağlarında güvenin kritik rolü vurgulanmakta ve Blockchain merkezi olmayan yapısının katılımcılar arasındaki güveni nasıl sağladığına dikkat çekilmektedir. Ek olarak, Blockchaindeki belirsiz sistemlerin ortaya çıkardığı ve gelişen güvenlik endişelerini kapsayabilecek zorluklara işaret etmektedir. Katılımcılar bu temaların kapsamlı bir şekilde incelenmesini ve Blockchainin potansiyel belirsizlik durumlarıyla başa çıkarken güvenlik ve güvenilirliği nasıl sağladığının daha iyi anlaşılmasını bekleyebilirler.

Blockchain Teknolojisi Ne Kadar Güvenli?

Blockchain teknolojisi genellikle kurcalamaya dayanıklı ve dağıtılmış defter özellikleri nedeniyle övülüyor. Ancak hiçbir sistemin tamamen güvenli olmadığını unutmamak önemlidir. Verilerin güvenliğini sağlamak için Blockchain güvenliğinin temellerini anlamak çok önemlidir. Blockchain'in en önemli avantajlarından biri merkezi olmayan kontrole izin vermesidir. Saldırıya uğrayabilecek veya

çevrimdışına alınabilecek merkezi bir otorite yoktur. Bunun yerine ağ, her biri Blockchain'in bir kopyasını saklayan düğümlerden oluşur.

Bir bilgisayar korsanının Blockchain'i kurcalaması için ağdaki her bir düğümü hacklemesi gerekir; bu son derece zor bir başarıdır. Blockchain'in bir diğer önemli güvenlik özelliği de kriptografik karmadır. Bu, zincirdeki her bloğun benzersiz bir şekilde tanımlanmasına ve bir önceki bloğa bağlanmasına olanak tanır. Blockchain teknolojisi güvenlik açısından oldukça etkileyicidir. Ancak hiçbir sistem tamamen aşılmaz değildir. Blockchain'de de bazı güvenlik açıkları bulunabilmektedir. Bu nedenle dikkatli olmak önemlidir. Son olarak verilerinizi korumak için daha detaylı olarak anlatıldığı gibi temel güvenlik önlemlerini almanız önemlidir.

Peki ya güvenlik ve gizlilik?

Geleneksel bilgi sistemlerinde hem sağlam güvenlik hem de sarsılmaz gizlilik elde etmek zor olabilir. Bu, büyük bir sorumluluktur. Yine de, doğru stratejiler ve çözümlerle bu zorlukların üstesinden gelebiliriz. Ancak blockchain, ustaca bir çözüm sunarak bir umut ışığı olarak ortaya çıkmaktadır. Bu hassas dengeleme işlemini "açık anahtar altyapısı" olarak bilinen ve verileri kurcalamaya yönelik her türlü kötü niyetli girişime karşı bir kalkan görevi gören bir kavramı devreye sokarak gerçekleştirir. Ek olarak, Blockchain defterin boyutunu koruyarak veri gizliliğini daha da güçlendirir. İlginç bir şekilde, Blockchain güvenliğinin gücünün, ağının büyüklüğü ve dağılımı ile arttığına inanılmaktadır.

Ancak, çığır açan her teknoloji gibi, Blockchain de kendi endişelerini beraberinde getirmektedir. Bu endişelerden bazıları ölçeklenebilirlik sınırlamaları, veri gizliliğinin korunmasındaki zorluklar ve standartlaştırılmış endüstri uygulamalarının olmamasıdır.

Özellikle Genel Veri Koruma Yönetmeliği'nin (GDPR) katı düzenlemeler getirdiği Avrupa Birliği'nde (AB), veri gizliliği özellikle çetrefilli bir konudur. Mayıs ayından bu yana yürürlükte olan bu düzenlemeler, rıza ve veri saklama konusunda katı koşullar getirmektedir. İşletmeler artık işlemler sırasında AB vatandaşlarının kişisel verilerini ve gizliliğini koruma sorumluluğuyla karşı karşıya. Ayrıca GDPR, kişisel verilerin AB dışına aktarılmasını yasaklayarak vatandaşlara "tüm verileri üzerinde tam ve nihai kontrol" yetkisi veriyor.

Bu durum, hem düğüm ana bilgisayarları üzerinde kontrol sahibi olmayan halka açık Blockchainler hem de genellikle izinli Blockchainleri olarak adlandırılan özel blok zincirleri için benzersiz bir zorluk teşkil etmektedir. Yani bu ortamlarda veriler silinemez. Dahası, GDPR, blok zincirinin savunduğu "işlemlerin değişmezliği" ile çelişen bir kavram olan "unutulma hakkını" getirmektedir.

Blockchain; güvenlik, gizlilik ve mevzuata uygunluk talepleriyle boğuşurken, bu karmaşık ortamda gezinmek yenilikçi çözümler gerektirmektedir. Sürekli gelişen bir teknoloji olan blockchain dünyasında bu yönleri uyumlu hale getirme yolculuğu karmaşık ama bir o kadar da önemli bir çabadır.

Blockchain Türleri ve Güvenlik Tehditleri

Gelecekteki Sandbox projeleri yapay zeka (AI) ile daha akıllı ve etkileşimli hale gelebilirler. Örneğin, oyun içi karakterleri kontrol eden yapay zeka ve oyuncuların gerçekçi ve dinamik deneyimler yaşadığı oyunlar geliştirilebilirler. Oyuncuların Yapay Zeka ile etkileşime girerek farklı senaryoları deneyimlemelerine olanak sağlar.

4 tür Blockchain vardır:
Halka Açık Blockchain

Bitcoin gibi halka açık Blockchain kapılarını herkese açar. Herkesin işlem geçmişlerine göz atabileceği ve yenilerini oluşturabileceği kapsayıcı bir alandır. Bu Blockchain ademi merkeziyetçilik ve güvenliğin somutlaşmış halidir, ancak bunun bir bedeli vardır – yavaş ve pahalı olabilirler.

Halka açık Blockchainlerin güzelliği erişilebilir olmalarında yatar. Herkese açık olmaları, tehditlere karşı genellikle daha sağlam oldukları anlamına gelir. Aslında halka açık bir blok zincirine %51'lik bir saldırı gerçekleştirmeye çalışmak, bu zincirin özel muadiline kıyasla samanlıkta iğne aramaya benzer.

Özel Blockchain

Özel bir Blockchain zincirini, yalnızca davet edilen üyelerin verilere ve işlem ayrıcalıklarına erişebildiği özel bir kulüp olarak düşünün. Bu blok zincirleri genellikle izinlidir, yani kimin gireceğine merkezi bir otorite karar verir.

Özel Blockchain zincirlerinin cazibesi gizlilik ve hızdır. Verilere erişen seçkin bir grupla, bilgisayar korsanlığı girişimleri daha zor hale gelir. İşlemler mi? Herkesin katılmasını beklemeye gerek olmadığı için ağda herkese açık blok zincirlerinden daha hızlı ilerlerler.

Ancak, bir sorun var. Özel Blockchainler bazen güvenlik konusunda soru işaretlerine yol açıyor. Özel Blockchainler güvenlik için tek bir varlığa dayanırlar. Yani bu varlık tökezler ise tüm ağ çökebilir.

Hibrit Blockchain

Hem kamusal hem de özel dünyanın en iyi yönlerini bir araya getiren bir Blockchain hayal edin. Öyleyse Hibrit Blockchain zincirine hoş geldiniz. Sonuç olarak kullanıcılar Blockchaine kimlerin gireceğini ve hangi işlemlerin halka açık olacağını belirleme gücüne sahiptir.

Bu ince bir dengeleme hareketidir. Peki ya artı tarafı nedir? Hem genel hem de özel Blockchainlerin avantajlarını elde edersiniz. Ancak herkesin tercihlerini takip etmek merkezi otorite için zor olabilir.

Güvenliği desteklemek için birçok saygın web sitesi ücretsiz blockchain güvenlik sertifikaları sunmaktadır. Böylece kullanıcıları temel güvenlik bilgi ve becerileriyle donatırlar.

Konsorsiyum Blockchain

Konsorsiyum Blockchainleri, merkezi bir otoritenin onay damgası sayesinde fikir birliği masasında yer almayı hak eden tanınmış katılımcılara ev sahipliği yapmaktadırlar. Şimdi arka uç işlemlerini kolaylaştırmak için bir konsorsiyum Blockchaini paylaşan bir grup bankayı hayal edin. Peki ya avantajı nedir? Yalnızca güvenilir oyuncular hassas verilere girebilirler. Böylece güvenlikten ödün vermeden verimliliği artırırlar. Güvenlikten bahsetmişken, konsorsiyum Blockchainleri güvenlik spektrumunda kamu ve özel arasında bir yerde yer alır. Halka açık olanlar kadar sağlam olmayabilirler ancak özel olanlara göre daha fazla güvenlik sunarlar. Blockchain dünyası çözüldüğünde, her türün kendine özgü cazibeleri ve zorlukları olduğu açıktır. Aslında önemli olan, güvenlik ve verimliliği akılda tutarken ihtiyaçlarınıza en uygun olanı seçmektir.

Blockchain Teknolojisinin Temelleri: Blockchain Uygulamaları ve Kullanım Durumları

Bu bölümde, dijital sanatta blok zinciri teknolojisinin farklı operasyonlarını ve kullanım alanlarını keşfediyoruz. Öğreniciler Blockchain in finans, kuvvet zinciri operasyonları, sağlık hizmetleri ve diğer sektörlerde nasıl uygulandığını inceleyecekler. Artan saydamlık, etkinlik veya azalan maliyetler de dahil olmak üzere Blockchain in dolaylı faydaları hakkında algı kazanacaklar. Ayrıca öğrenciler, Blockchainin performansa nasıl dönüştüğünü anlayabilmek için gerçek dünya örnek olaylarını inceleyeceklerdir.

Blockchain teknolojisinin en iyi uygulamaları nelerdir?

Aslında Blockchain teknolojisi hemen hemen her sektörde kullanılıyor: Blockchain teknolojisi, güvenlik, şeffaflık ve merkeziyetsizlik gibi temel ilkeleriyle çok sayıda sektörü dönüştürüyor. İşte Blockchain teknolojisinin en iyi uygulamalarından bazıları:

1.Kripto para birimi:

Bitcoin ve Ethereum gibi kripto para birimleri Blockchain teknolojisinin belki de en önde gelen uygulamaları arasında yer alıyor. Bankalar gibi aracılara ihtiyaç duymadan güvenli, kişiler arası dijital işlemlere olanak sağlarlar. Kripto para birimleri küresel finans sisteminde devrim yaratma potansiyeline sahiptir.

2. Sağlık Hizmetleri:

Blockchain, elektronik sağlık kayıtlarını güvenli bir şekilde yöneterek sağlık sektöründe devrim yaratma potansiyeline sahiptir. Hastalar tıbbi verileri üzerinde daha fazla kontrol sahibi olurken, sağlık hizmeti sağlayıcıları da veri bütünlüğü veya güvenliğini sağlarken kayıtlara daha verimli bir şekilde erişebilir ve bunları güncelleyebilirler.

3. Finans ve Bankacılık:

Finans ve Bankacılık sektöründe blockchain önemli adımlar atıyor. Daha hızlı, daha güvenli ve uygun maliyetli sınır ötesi ödemeler ve havaleler sunuyorlar. Sonuçta ticaret finansmanı, ödeme sistemleri ve dolandırıcılığın azaltılmasında Blockchain kullanım oranı artıyor.

4. Gayrimenkul:

Gayrimenkul sektörü, emlak işlemlerini basitleştirmek için Blockchainden yararlanıyorlar. Yani mülk sahipliği geçmişinin şeffaf bir defterini sağlayarak alım satım süreçlerinde sahtekarlığı azaltıyor ve paydaşlar arasında güveni artırıyor.

5. Perakende:

Perakendeciler tedarik zinciri şeffaflığını artırmak için Blockchain teknolojisini araştırıyor. Böylece tüketiciler, ürünlerin nereden geldiğini takip ederek kaliteli ve etik kaynak kullanımını sağlayabilirler. Bu şeffaflık, tüketiciler veya markalar arasında güven oluşturabilecektir.

6. Tedarik Zinciri ve Lojistik:

Blockchain, tedarik zinciri boyunca malların şeffaflığını ve izlenebilirliğini artırır. Yani şirketler ürünleri kaynağından tüketiciye kadar takip eder, sahte mal riskini azaltır ve lojistik operasyonlarını kolaylaştırır.

7. Sigorta:

Sigorta sektöründe blockchain, akıllı sözleşmeler aracılığıyla talep işlemlerini otomatikleştirebilir. Böylece, idari maliyetleri azaltır ve talep sürecinde şeffaflığı artırır. Sigorta poliçesi sahipleri daha hızlı ve daha isabetli tazminat talepleriyle karşılaşırlar.

8. Oylama ve Yönetişim:

Blockchain teknolojisi oylama ve yönetişim sistemlerinde devrim yaratma potansiyeline sahiptir. Güvenli ve müdahaleye karşı korumalı dijital oylama sağlayabilir, seçmen katılımını artırabilir veya seçim sonuçlarına olan güveni oluşturabilir. Blockchain tabanlı yönetişim modelleri de karar alma süreçlerinde şeffaflığı artırabilirler.

9. Nesnelerin İnterneti (IoT):

Nesnelerin İnterneti (IoT) ortamı genişlemeye devam ettikçe, blockchain IoT cihazları tarafından üretilen büyük miktarda veriyi güvence altına alabilirler. Böylece, cihazlar arasında güvenli iletişim sağlar ve bilgisayar korsanlığı ve veri ihlalleri riskini azaltır.

10. Medya ve Reklamcılık:

Medya ve reklamcılık sektörleri şeffaflığı artırmak ve dolandırıcılığı azaltmak için Blockchaini benimsiyor. Reklam verenler, reklamlarının doğru kitleye ulaştığından emin olabilirler. Böylece içerik oluşturucular ise adil bir tazminat alabilirler.

İşletmeler, genellikle bir hizmet sağlayıcı olarak Blockchain tarafından barındırılan Blockchain platformları aracılığıyla dijital ödemeler veya tedarik zincirleri gibi herhangi bir amaç için Blockchain

uygulamaları oluşturabilir. Bu dağıtık defter teknolojisi (DLT), herkes için güven ve güvenlik tesis ederek dijital ekonomide çalışma şeklimizi yeniden tanımlamaktadır.

Bunlar, Blockchain teknolojisinin temelleri nin çeşitli sektörlerde nasıl iz bıraktığına dair sadece birkaç örnek. Temelinde yatan güvenlik, şeffaflık ve merkeziyetsizlik ilkeleri sektörleri yeniden şekillendiriyor. Ayrıca asırlık zorluklara yeni çözümler sunuyorlar. Son olarak Blockchain gelişmeye devam ettikçe, muhtemelen uygulamaları genişleyecek ve hayatımızın çok daha fazla yönünü etkileyecektir.

Blockchain Teknolojisinin Temelleri: Referanslar ve Kaynaklar

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

2. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin. https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf

3. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media. https://www.oreilly.com/library/view/blockchain/9781491920480/

4. Antonopoulos, A. M. (2017). Mastering Bitcoin: Unlocking digital cryptocurrencies. O'Reilly Media. http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/7829/1/Mastering%20Bitcoin_%20Programming%20the%20Open%20Blockchain.pdf

5. World Economic Forum. (2018). Blockchain beyond the hype: A practical framework for business leaders. Retrieved from https://www.weforum.org/whitepapers/blockchain-beyond-the-hype-a-practical-framework-for-business-leaders

6. Kasey Panetta, What is blockchain? Gartner, September 23, 2019, https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain

Co-funded by
the European Union

Blockchain Alanındaki Temel Güvenlik Endişeleri

Bu blog yazısını AB tarafından finanse edilen “V2B: Sanat Mesleki Eğitim Kursiyerleri için Metaverse’de NFT Fırsatları Yaratmak” projesi için oluşturduk ve proje referans numaramız 2022-1-DE02-KA210-VET-000080828. L4Y Learning for Youth GmbH tarafından Adana Çukurova Güzel Sanatlar Lisesi ve EMC Services Ltd işbirliğiyle koordine edilen “Blockchain Alanındaki Temel Güvenlik Endişeleri” giriş yazısındaki eğitim çerçevesiyle ilgili olarak hazırlanmıştır.

Blockchain teknolojisinin iki önemli boyutu vardır: dağıtık mutabakat ve anonimlik ve dijital olarak (çevrimiçi) değiş tokuş edilen herhangi bir dijital varlık işlemi için geçerlidir. Dağıtık mutabakat modelinden yararlanarak gelecekte herhangi bir noktada doğrulayarak dijital işlemlerde (geçmiş veya şimdiki) devrim yaratma potansiyeline sahiptir. Blok zinciri teknolojisinden büyük beklentiler olmasına rağmen, yaygın olarak benimsenmesine yol açan zorlukları, potansiyel fırsatları ve uygulamaları anlamak için yeterli bilgi bulunmamaktadır1.

Blockchain teknolojisi, kripto para birimleri, tedarik zinciri yönetimi, dijital kimlikler ve daha fazlası dahil olmak üzere çeşitli uygulamalar için merkezi olmayan ve güvenli bir sistem olarak büyük bir popülerlik kazanmıştır Blockchain çeşitli avantajlar sunar, ancak güvenlik endişelerine karşı bağışık değildir. Teknoloji geliştikçe, bütünlüğünü tehlikeye atabilecek tehditler ve güvenlik açıkları ortaya çıkmaktadır. Bu modül, blok zinciri alanındaki bazı temel güvenlik endişelerini ele almaktadır. Bu yazı, gelişmekte olan teknolojiler, dijital buluşlar ve çevrimiçi ilişkilerin geleceği ile ilgilenen öğrenciler için hazırlanmıştır. R2 kategorimizde daha fazla blog yazısı da bulabilirsiniz. Bu yayınlardan biridir.

Blockchain Alanındaki Temel Güvenlik Endişeleri: Öğrenme Hedefleri

Blockchain Teknolojisinin Temellerini Anlamak

Blockchainin Güvenliği Konusunda Farkındalık Kazanmak

51% Saldırılarının ve Mutabakat Mekanizmalarının Gözden Geçirilmesi

Akıllı Sözleşme Güvenliği Konusunda Farkındalığın Artırılması

Gizlilik Konularının Gözden Geçirilmesi

Farklı Blockchain Ağları Arasındaki Etkileşimi Anlamak

Co-funded by
the European Union

Blockchain Alanındaki Temel Güvenlik Endişeleri: Giriş

Üniteye blok zincirinin ne olduğunu açıklayarak başlamak uygun olacaktır. Blok zinciri, tek bir taraf yerine bir bilgisayar ağı tarafından yönetilen paylaşılan bir veritabanıdır. Bu merkezi olmayan yapı daha fazla şeffaflık ve güvenlik sağlar, çünkü zincirdeki her bir taraf her işlemi blok zincirinin tüm geçmişine karşı doğrulayabilir.

Blok zincirinin nasıl çalıştığını anlamanın anahtarı, onu dijital bir defter olarak düşünmektir. Geleneksel defterlerde banka ya da hükümet gibi merkezi bir otorite işlemleri kaydeder ve denetler. Buna karşılık, blok zincirleri merkezi değildir, yani defteri yöneten merkezi bir otorite yoktur. Bunun yerine, defter zincirdeki tüm taraflar arasında paylaşılır ve ayrıştırılır.

Her yeni işlem gerçekleştiğinde, bu işlem blok zincirine kaydedilir. Zincirdeki tüm taraflar daha sonra bu işlemleri doğrulamak için gelişmiş matematiksel algoritmalar kullanır. Bir işlem doğrulandıktan sonra değiştirilemez veya silinemez. Bu, blok zincirinde gerçekleşen tüm işlemlerin kalıcı ve güvenli bir kaydını oluşturur.2

Blok zinciri teknolojisine yönelik saldırıların nasıl gerçekleştiğine bir göz atalım: Blok zinciri ve veri güvenliği kullanıcılar için her zaman endişe verici bir konudur. Blockchain teknolojisi de güvenlik açıklarıyla ilgilenir ve dört tür saldırıya karşı savunmasızdır: kimlik avı, yeniden yönlendirme, Sybil ve %51 saldırıları.

1. Kimlik avı

Kimlik avı saldırısı, bir saldırganın mağdurları kandırarak oturum açma bilgileri veya finansal bilgiler gibi hassas bilgileri ifşa etmelerini sağlamak amacıyla güvenilir bir kuruluşun kimliğine büründüğü bir siber saldırı türüdür. Yani bu kimlik avı saldırıları genellikle kurbanları meşru borsalar veya cüzdanlar gibi görünecek şekilde tasarlanmış kötü niyetli web sitelerine yönlendiren sahte bağlantılar göndererek kurbanlardan kripto para çalmak için kullanılır.

Bu web siteleri daha sonra kullanıcıdan giriş bilgilerini girmesini isteyecek ve saldırgan da bu bilgileri kullanarak hesaplarına erişip kripto paralarını çalabilecektir. Bu nedenle birçok farklı ülkede blockchain güvenlik maaşları yüksektir çünkü mühendisler ve geliştiriciler kimlik avından kaçınmak için gerçekten çok çalışmak zorundadır.

Kimlik avı, saldırganların insanları kandırarak kullanıcı adları, şifreler ve kredi kartı bilgileri gibi hassas bilgileri ifşa etmeye çalıştığı bir siber saldırı türüdür. Bu genellikle bir banka veya sosyal medya platformu gibi meşru bir kaynaktan geliyormuş gibi görünen sahte e-postalar veya mesajlar aracılığıyla yapılır. Kimlik avının amacı, kimlik hırsızlığı veya finansal kazanç için kullanılabilecek kişisel bilgileri çalmaktır. Kimlik avı dolandırıcılığının kurbanı olmamak için, bilinmeyen gönderenlerden gelen e-postaları veya mesajları açarken dikkatli olmak önemlidir. Kişisel bilgi taleplerine karşı dikkatli olun ve şüpheli kaynaklardan gelen bağlantılara asla tıklamayın veya ekleri indirmeyin. Bilgisayarınızı ve mobil cihazlarınızı en son güvenlik yamaları ve antivirüs yazılımları ile güncel tutmanız da önemlidir.

Şüpheli bir e-posta veya mesaj alırsanız, yanıt vermeyin veya herhangi bir bağlantıya tıklamayın. Bu mesajı ilgili makamlara bildirin ve gelen kutunuzdan silin.

2. Yönlendirme Saldırısı

Blok zinciri teknolojisinde meydana gelebilecek bir diğer saldırı türü de yönlendirme saldırısıdır. Bu, bilgisayar korsanlarının internet servis sağlayıcılarına aktarılırken verilere müdahale etmesidir. Bunu yaparak ağı bozabilir ve işlemlerin tamamlanmasını engelleyebilirler. Yönlendirme saldırısı, bir saldırganın meşru bir yönlendirici gibi davranarak sahte yönlendirme güncellemeleri gönderdiği bir siber saldırı türüdür. Bir başka yönlendirme saldırısı türü de kaynak yönlendirme saldırısı olarak adlandırılır ve burada bir paketin göndericisi, paketin ağ üzerinden geçeceği rotayı belirler.

Yönlendirme saldırılarını tespit etmek ve önlemek zor olabilir, ancak alınabilecek bazı önlemler vardır. Örneğin, veriler gönderilmeden önce şifrelenebilir ve düğüm operatörleri ağlarını şüpheli etkinliklere karşı izleyebilir.

Bu tür saldırıların farkında olmak ve kendinizi ve ağınızı korumak için uygun önlemleri almak önemlidir. Bu riskleri azaltmanın bazı yolları arasında yazılımınızı güncel tutmak, güçlü parolalar kullanmak ve bilinmeyen gönderenlerden gelen e-postaları veya mesajları açarken dikkatli olmak yer alır.

3. Sybil Saldırısı

Sybil saldırısı, bilgisayar korsanlarının ağı kalabalıklaştırmak ve sistemi çökertmek için birçok sahte kimlik oluşturup kullandığı bir tür blok zinciri saldırısıdır. Bu, birden fazla hesap, bilgisayar veya kimlik oluşturularak yapılabilir. Sybil saldırıları blok zincirine olan güveni azaltabileceği gibi finansal kayıplara da yol açabilir. Bir Sybil saldırısını önlemek için güçlü güvenlik önlemlerinin alınması önemlidir. Bu önlemler arasında dijital imzaların ya da kimliklerin kullanılması ve bilinen kimliklerin bir listesinin tutulması yer alabilir.

Bir Sybil saldırısının risklerini azaltmak için kimlik doğrulama ve itibar sistemleri gibi uygun güvenlik önlemlerinin uygulanması önemlidir. Ayrıca kullanıcıları Sybil saldırılarının riskleri ve kendilerini bu tür saldırılardan nasıl koruyacakları konusunda eğitmek de önemlidir.

4. %51 Saldırısı

%51 saldırısı, bir grup madencinin veya tek bir madencinin ağın madencilik gücünün %50'sinden fazlasını kontrol ettiği bir tür blockchain saldırısıdır. Bu kontrol, defterleri manipüle etmelerine olanak tanıyor ve bu da çifte harcamaya veya diğer dolandırıcılık türlerine yol açabiliyor. %51 saldırıları çok nadir olmakla birlikte, blockchain güvenliği açısından ciddi bir güvenlik endişesidir. Bunlara karşı korunmak için blockchain ağlarının büyük ve merkezi olmayan bir madencilik topluluğuna sahip olması önemlidir. %51 saldırısı risklerini azaltmak için kimlik doğrulama ve itibar sistemleri gibi uygun güvenlik önlemlerinin uygulanması önemlidir.

Bunlar Blockchain siber güvenliğini etkileyebilecek ve zarar verebilecek birçok yoldan sadece birkaçı. (1)

Blockchain Alanındaki Güvenlik Endişeleri için İpuçları ve En İyi Uygulamalar

Herkes için geçerli olan belirli Blockchain güvenlik ipuçları ve uygulamaları vardır:

1. İki Faktörlü Kimlik Doğrulamasının Uygulanması

Blockchain alanındaki güvenlik endişeleri 'ni önlemenin en önemli yönlerinden biri iki faktörlü kimlik doğrulamadır (2FA). 2FA'yı uygulamak, oturum açmak için şifrenize ek olarak ikinci bir faktör gerektirerek çevrimiçi hesaplarınıza ekstra bir güvenlik katmanı ekler. Bir donanım belirteci, parmak iziniz veya iris taramanız gibi biyometrik bir faktör veya bir kimlik doğrulama uygulaması tarafından oluşturulan tek seferlik bir kod bu ikinci faktör olarak kullanılabilir.

2FA kusursuz olmasa da, çevrimiçi hesaplarınızın güvenliğini önemli ölçüde artırır ve mümkün olduğunda kullanılmalıdır. Blok zinciri alanında, dijital varlıkların yüksek değeri ve bir hack veya hırsızlığın neden olabileceği genellikle onarılamaz hasar nedeniyle 2FA özellikle önemlidir. Ayrıca, sistemdeki herhangi bir boşluğu tespit edebilecek ve güvenlik açıklarını ortadan kaldırabilecek saygın blok zinciri güvenlik denetim şirketleri bulmaya çalışın.

İki faktörlü kimlik doğrulama (2FA), geleneksel şifrelere başka bir güvenlik katmanı ekleyen gelişmiş bir kullanıcı kimlik doğrulama yöntemidir. İşte 2FA'yı uygulamak için bazı adımlar:

- Doğru teknolojiyi seçin: SMS tabanlı kimlik doğrulama, mobil uygulamalar ve donanım belirteçleri gibi çeşitli 2FA teknolojileri mevcuttur. İhtiyaçlarınıza ve bütçenize en uygun olanı seçin.
- Kullanıcıları eğitin: Kullanıcıları 2FA'nın faydaları ve nasıl kullanılacağı konusunda eğitmek önemlidir. Başlamalarına yardımcı olmak için açık talimatlar ve eğitim materyalleri sağlayın.

- Kullanımı kolay hale getirin: 2FA'nın kullanımı kolay olmalı ve kullanıcılar için ek yük oluşturmamalıdır. Kullanıcıların bir kez oturum açmasına ve birden fazla uygulamaya erişmesine olanak tanıyan çoklu oturum açma (SSO) çözümlerini kullanmayı düşünün.
- Kullanımı izleyin: 2FA'nın doğru ve etkili bir şekilde kullanıldığından emin olmak için kullanımını izleyin. Herhangi bir sorunu veya iyileştirme alanını belirleyin ve bunları derhal ele alın.
- Güncel kalın: En son güvenlik tehditlerini ve güvenlik açıklarını takip edin ve 2FA teknolojinizi buna göre güncelleyin.

2FA'nın nasıl uygulanacağı hakkında daha fazla bilgi için bu Microsoft Güvenlik Blogu makalesine göz atın(3).

2. Güvenilir Gönderenlerin ve Alıcıların Listelenmesine İzin Verin

Blockchain platformunuzun güvenliğini sağlamak için yapabileceğiniz en iyi şeylerden biri, yalnızca güvenilir gönderici ve alıcılara izin vermektir. Bu zahmetsiz gibi görünebilir, ancak inanılmaz derecede önemlidir. Yalnızca güvenilir varlıkların blok zinciri ile etkileşime girmesine izin vererek kötü niyetli faaliyet olasılığını önemli ölçüde azaltabilirsiniz. Elbette bu, Blockchaine yeni varlıkların girmesine asla izin vermemeniz gerektiği anlamına gelmez.

Aksine, sadece kime erişim izni verdiğiniz konusunda çok dikkatli olmanız gerektiği anlamına gelir. Her bir gönderici ve alıcının kimliğini doğrulamak için zaman ayırın ve ağa girmelerine izin vermeden önce güvenilir olduklarından emin olun.

Kullanıcıların güvenilir gönderenleri ve alıcıları listelemesine izin vermek, kimlik avı dolandırıcılıklarına ve diğer siber saldırılara karşı korunmaya yardımcı olabilecek bir güvenlik önlemidir. İşte bu önlemi uygulamanın bazı yolları:

- Kullanıcı İzin Verme/Engelleme Listesi: Bu, güvenilir gönderenlerden veya etki alanlarından gelen postalara izin vermek için en çok önerilen seçenektir. Sahte göndericiler de dahil olmak üzere etki alanları ve e-posta adresleri için izin girişleri oluşturabilirsiniz.
- Posta akış kuralları: Posta akış kuralları, güvenilir gönderenlerden gelen iletileri tanımlamak ve uygun eylemleri gerçekleştirmek için kullanılabilir.
- Outlook Güvenli Gönderenler: Outlook'taki Güvenli Gönderenler listesi, güvendiğiniz e-posta adreslerini veya etki alanlarını eklemek için kullanılabilir .
- IP İzin Verilenler Listesi: IP İzin Verme Listesi, belirli IP adreslerinden veya aralıklarından gelen e-postalara izin vermek için kullanılabilir.

Posta listeleri: Güvenilir kaynaklardan e-posta aldığınızdan emin olmak için güvenli gönderenler listenize posta listeleri ekleyebilirsiniz.
Kullanıcıları kimlik avı dolandırıcılığı ve diğer siber saldırıların riskleri ve kendilerini bu tür saldırılardan nasıl koruyacakları konusunda eğitmek önemlidir. Bu güvenlik önlemlerinin nasıl uygulanacağı hakkında daha fazla bilgi için bu Microsoft Learn makalesine göz atın(4).

3. Yazılımınızı Güncel Tutun

Bu, güvenlik güncellemelerini yüklemek ve herhangi bir güvenlik açığını keşfeder keşfetmez düzeltmek anlamına gelir. En son güvenlik tehditlerini takip ederek blockchain ağınızın güvenli ve güvenli kalmasını sağlamaya yardımcı olabilirsiniz. Ayrıca blockchain güvenlik ihtiyaçlarınız için saygın ve güvenilir bir sağlayıcı seçmeniz önemlidir. Ağlarını güvende ve emniyette tutma konusunda kanıtlanmış bir geçmişe sahip bir sağlayıcı arayın.

Yazılımınızı güncel tutmak, bilgisayarınızı güvenlik tehditlerinden korumanın önemli bir adımıdır. Yazılım güncellemeleri genellikle olası saldırıları engelleyen ve uygulamalara ve verilere yetkisiz erişimi önleyen güvenlik yamaları ve düzeltmeleri içerir. Yazılımınızı güncel tutmak için atabileceğiniz bazı adımlar şunlardır:

- Otomatik güncellemeleri etkinleştirin: Çoğu yazılım uygulamasında otomatik güncellemeleri etkinleştirme seçeneği bulunur. Bu, herhangi bir manuel müdahaleye gerek kalmadan yazılımınızın her zaman güncel olmasını sağlayacaktır.

- Güncellemeleri düzenli olarak kontrol edin. Otomatik güncellemeler mevcut değilse güncellemeleri düzenli olarak kontrol ettiğinizden emin olun. Bu genellikle uygulamanın ayarları veya tercihler menüsü aracılığıyla yapılabilir.
- Güncellemeleri güvenilir kaynaklardan indirin: Yazılım güncellemelerini indirirken bunları yazılım satıcısının resmi web sitesi gibi güvenilir kaynaklardan indirdiğinizden emin olun.
- İşletim sisteminizi güncel tutun: Yazılımınızı güncel tutmanın yanı sıra, işletim sisteminizi en son güvenlik yamaları ve güncellemelerle güncel tutmanız da önemlidir.
- Kullanılmayan yazılımları kaldırın: Kullanılmayan yazılımları kaldırmak, bilgisayarınızın saldırı yüzeyini azaltmaya ve güvenlik ihlali riskini en aza indirmeye yardımcı olabilir.

4. VPN Kullanma – Sanal Özel Ağ

VPN'lerin kullanımı yeni olmasa da, çevrimiçi güvenlik tehditlerine ilişkin farkındalığın artması nedeniyle popülerlik kazanmaktadır. VPN, iki cihaz arasında güvenli, şifreli bir bağlantıdır. Bu bağlantı, veri trafiğini internet gibi güvenilmeyen bir ağ üzerinden aktarabilir.

VPN, veri trafiğini şifreleyerek bilgilerinizin kötü niyetli aktörlerden korunmasına yardımcı olabilir. Ayrıca VPN, gerçek IP adresinizi ve konumunuzu gizleyerek gizliliğinizi artırmanıza da yardımcı olabilir. Aralarından seçim yapabileceğiniz pek çok farklı VPN sağlayıcısı olsa da, güçlü şifreleme ve güvenlik özelliklerine sahip saygın bir sağlayıcı seçmek önemlidir.

Sanal özel ağ (VPN), cihazınız ile internet arasında güvenli ve şifreli bir bağlantı oluşturan bir hizmettir. VPN'ler, IP adresinizi gizleyerek, internet trafiğinizi şifreleyerek ve üçüncü tarafların çevrimiçi etkinliklerinizi izlemesini engelleyerek çevrimiçi gizliliğinizin ve güvenliğinizin korunmasına yardımcı olabilir. VPN kullanmanın bazı yararları şunlardır:

- Çevrimiçi gizlilik: VPN, IP adresinizi gizleyerek ve internet trafiğinizi şifreleyerek çevrimiçi gizliliğinizin korunmasına yardımcı olabilir. Bu, üçüncü tarafların çevrimiçi etkinliklerinizi izlemesini zorlaştırır.
- Güvenlik: VPN, internet trafiğinizi şifreleyerek ve bilgisayar korsanlarının verilerinizi ele geçirmesini önleyerek çevrimiçi güvenliğinizin korunmasına yardımcı olabilir.
- Kısıtlanmış içeriğe erişim: VPN, coğrafi kısıtlamaları atlamanıza ve bölgenizde engellenebilecek içeriğe erişmenize yardımcı olabilir.
- Herkese açık güvenli Wi-Fi: VPN, internet trafiğinizi şifreleyerek ve başkalarının verilerinize müdahale etmesini önleyerek genel Wi-Fi ağlarında güvende kalmanıza yardımcı olabilir.
- Uzaktan erişim: VPN, özel bir ağdaki kaynaklara uzak bir konumdan güvenli bir şekilde erişmenize olanak tanır.

VPN sağlayıcı seçerken hız, güvenlik, gizlilik politikası ve kullanım kolaylığı gibi faktörleri dikkate almak önemlidir.

5. Kimlik Avı Koruması Araçlarını Kullanın

Kimlik avı saldırıları giderek yaygınlaşıyor ve tespit edilmesi ve önlenmesi zor olabiliyor. Yani kimlik avına karşı koruma aracı, kimlik avı girişimlerini tanımlamanıza ve engellemenize yardımcı olarak blok zincirinizi güvende tutar. Ayrıca, kimlik avı saldırısının işaretlerinin farkında olmak da önemlidir. Sizden bir bağlantıya tıklamanızı veya kişisel bilgilerinizi vermenizi isteyen herhangi bir e-posta veya mesajdan şüphelenin. Bir e-postanın meşruluğu konusunda şüpheniz varsa, orijinalliğini doğrulamak için gönderenle iletişime geçin. (1)

Kimlik avı saldırıları, kimlik hırsızlığına, mali kayba ve diğer olumsuz sonuçlara yol açabilecek yaygın bir siber suç biçimidir. Kimlik avı önleme araçları, kimlik avı e-postalarını gelen kutunuza ulaşmadan önce tespit edip engelleyerek bu saldırılara karşı korunmanıza yardımcı olabilir.

Farklı düzeylerde koruma ve işlevsellik sunan birçok kimlik avı önleme aracı vardır.

Co-funded by
the European Union

Blockchain Alanındaki Temel Güvenlik Endişeleri

Blockchain teknolojisi son yıllarda oldukça popüler hale gelmiştir. Yani Blockchain dağınık bir defter sistemidir ve bu nedenle geleneksel veri tabanlarından çok daha güvenlidir. Bununla birlikte, blok zinciri teknolojisinin hala bazı güvenlik endişeleri vardır. Bu endişeler şunlardır:

Hacklenmeler: Blok zinciri ağları saldırılara karşı savunmasızdır. 2016 yılında DAO adlı bir Ethereum akıllı sözleşmesi hacklenmiş ve 50 milyon dolar değerinde kripto para çalınmıştır.5

DDoS saldırıları: Blockchain ağları DDoS saldırılarına karşı da savunmasızdır. DDoS saldırıları bir blok zinciri ağını yavaşlatabilir veya durdurabilir ve ağ üzerinde işlem yapmayı imkansız hale getirebilir.

Yanlış bilgilendirme: Blockchain teknolojisi kullanılarak yanlış bilgilerin yayılması mümkündür. Örneğin sahte sosyal medya paylaşımları veya haberler blok zincirinde saklanabilir.

Sansür: Blockchain sansür için kullanılabilir. Örneğin, bir hükümet blok zincirinde depolanan bilgileri sansürleyebilir.

Gizlilik: Blockchain gizlilik için bir tehdit oluşturabilir. Çünkü Blockchain tüm işlem geçmişini saklar. Bu da kullanıcıların finansal ve diğer hassas bilgilerini açığa çıkarabilir.

Blockchain Güvenlik Endişeleri: Sonuç

Bu güvenlik endişelerine rağmen, Blockchain teknolojisi hala çok güvenli bir teknolojidir. Geliştiriciler Blockchain ağlarını düzenli olarak güncelleyip iyileştirerek hacklenmeye karşı daha dirençli hale getirmektedir. Ayrıca geliştiriciler blok zinciri ağlarını DDoS saldırılarına karşı güçlendirecek eklentiler de yapmaktadır.

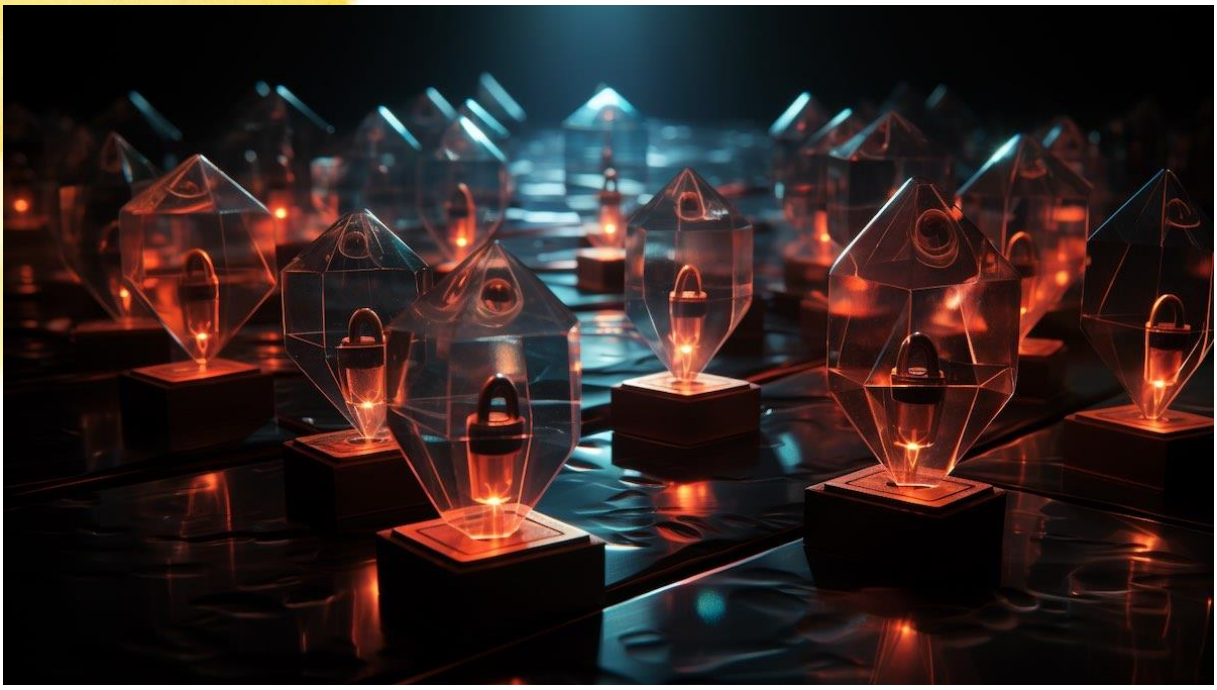
Blockchain teknolojisi daha yaygın bir şekilde kullanılmaya başlandıkça güvenlik endişeleri de artmaktadır. Ancak geliştiriciler Blockchain ağlarını sürekli güncelleyip geliştirerek daha güvenli hale getirmektedir.

Referanslar ve Kaynaklar

Upadhyay N., 2020 Demystifying blockchain: A critical analysis of challenges, applications and opportunities,International Journal of Information Management,Volume 54,102120, ISSN 0268-4012 ↩https://doi.org/10.1016/j.ijinfomgt.2020.102120
Blockchain Security – All You Need to Know ↩
https://www.microsoft.com/en-us/security/blog/2020/01/15/how-to-implement-multi-factor-authentication/ ↩
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/create-safe-sender-lists-in-office-365?view=o365-worldwide ↩

Co-funded by
the European Union

Güvenli Blockchain İşlemleri: Temel Stratejiler



Bu blog yazısını AB tarafından finanse edilen “V2B: Sanat Mesleki Eğitim Kursiyerleri için Metaverse’de NFT Fırsatları Yaratmak” projesi için oluşturduk ve proje referans numaramız 2022-1-DE02-KA210-VET-000080828. L4Y Learning for Youth GmbH koordinatörlüğünde Adana Çukurova Güzel Sanatlar Lisesi ve EMC Services Ltd işbirliğiyle “Güvenli Blockchain İşlemleri: Temel Stratejiler” başlıklı makale, giriş yazısındaki eğitim çerçevesiyle ilgili olarak hazırlanmıştır.

Bu makalede NFT’lerin (Non-Fungible Tokens) ve blok zinciri işlemlerinin güvenliğini sağlamaya yönelik stratejiler ele alınmaktadır. Yatırımlarınızı korumak ve hassas verileri güvende tutmak, özellikle dijital varlıklar ve bu teknoloji hızla büyürken son derece önemlidir. Mülkiyet haklarını güvence altına almak, siber tehditleri engellemek ve dijital varlıklarınızın bütünlüğünü korumak için bu makale, NFT’lerin ve blok zinciri işlemlerinin güvenliğini sağlamak için gerekli önlemleri kapsamaktadır.

Blok zinciri güvenliği, blok zincirlerindeki işlemleri ve dijital varlıkları korumak için gereklidir. Blok zinciri güvenlik stratejileri arasında şifreleme, mutabakat, değişmezlik, akıllı sözleşmeler ve siber saldırılara karşı savunma yer alır.

NFT’ler (Non-fungible token) blok zinciri teknolojisi ile oluşturulan benzersiz ve değiştirilemez dijital varlıklardır. NFT’lerin güvenliği, sahiplik haklarının korunmasını, veri bütünlüğünün sağlanmasını ve depolamanın güvence altına alınmasını içerir. NFT’ler siber korsanların hedefi olabilir, bu nedenle NFT’lerinizi saklamak için güvenilir bir kripto cüzdanı seçmeli ve kimlik avı saldırılarına karşı dikkatli olmalısınız. NFT’lerin mülkiyet haklarının korunması blockchain teknolojisi sayesinde mümkün hale geldi. NFT’ler, blockchain ağlarında depolanan, değiştirilemez tokenlardır. Bu tokenlar dijital varlıkların sahipliğini kanıtlar ve telif haklarını korur.

Güvenli Blockchain İşlemleri: Öğrenme Çıktıları

Bu modülün sonunda katılımcılar:

- NFT’lerin ve blok zinciri işlemlerinin güvenliğini sağlamanın önemini anlayacaklardır.
- Şifreleme, mutabakat ve akıllı sözleşmeler dahil olmak üzere blok zinciri güvenlik kavramlarını öğreneceklerdir.
- NFT’ler için güvenli depolama seçeneklerini tanımlayabileceklerdir.
- Kimlik avı risklerinin ve bunlara karşı nasıl korunulacağının farkında olacaklardır.
- Parola yönetimi ve iki faktörlü kimlik doğrulama dahil olmak üzere dijital varlıkların güvenliğini sağlamaya yönelik en iyi uygulamaları öğreneceklerdir.

- Uygulama indirmeleri ve sosyal medyada gizlilik için güvenilir kaynakların önemini anlayacaklardır.

NFT'lerin Mülkiyet Haklarını Korumak için Ne Gibi Önlemler Alabilirsiniz?

Güvenli Blockchain İşlemleri: Donanım Cüzdanı

NFT'lerinizi saklamak için bir donanım cüzdanı kullanın. Donanım cüzdanları, internete bağlı olmadıkları için yazılım cüzdanlarından daha yüksek güvenlik sunar.

Güvenilir donanım cüzdanlarına örnek olarak şunlar verilebilir:

Ledger

Trezor

KeepKey

BitBox

SafePal

Ellipal Titan

Coldcard Wallet

Bu cüzdanlar kripto para birimlerini güvenli bir şekilde saklamak için tasarlanmıştır. Her cüzdanın avantajları ve dezavantajları vardır. Bu nedenle kullanıcılar ihtiyaç ve tercihlerine göre en uygun kripto para cüzdanını seçmelidir.

Güvenli Blockchain İşlemleri: Güvenilir ve Lisanslı Platformlar

NFT ticareti yaptığınız platformların güvenilir ve lisanslı olduğundan emin olun. Platformların güvenlik sertifikalarını, kullanıcı yorumlarını ve destek hizmetlerini kontrol edin.

NFT ticareti yapmak isteyenler için birçok platform mevcuttur. Güvenli ve lisanslı NFT ticaret platformlarına örnek olarak aşağıdakiler verilebilir:

Binance NFT Marketplace

OpenSea

SuperRare

Rarible

Nifty Gateway

Foundation

MakersPlace

Bu platformlar, NFT ticareti yapmak isteyenler için güvenli ve lisanslı bir ortam sağlar. Bununla birlikte, her platformun kendine özgü avantajları ve dezavantajları vardır. Bu nedenle, kullanıcılar ihtiyaçlarına ve tercihlerine göre en uygun NFT ticaret platformunu seçmelidir.

E-dolandırıcılık

NFT ticareti yaparken kimlik avı saldırılarına dikkat edin. Kimlik avı saldırıları sahte e-postalar, SMS'ler veya web siteleri aracılığıyla kişisel bilgilerinizi veya cüzdan şifrenizi ister.

NFT'lerinizin değerini korumak için enflasyon ve nadirlik faktörlerini göz önünde bulundurun. NFT'lerinizin değeri piyasadaki arz ve talebe göre değişebilir. Nadir bulunan ve talep gören NFT'ler daha değerli olabilir.

Enflasyon ve Nadirlik

Enflasyon ve nadirlik faktörleri NFT'lerin değerinin korunmasında önemli bir rol oynar. Bu jetonların nadirliği, bir koleksiyon içindeki belirli bir değiştirilemez jetonun ayırt ediciliğini veya azlığını ifade eder. Koleksiyoncular nadir NFT'leri hevesle arar ve bu da genellikle bunların yüksek fiyatlardan satılmasına yol açar. Buna karşılık, NFT'ler alanındaki enflasyon, bir koleksiyondaki toplam NFT sayısının artmasıyla ilgilidir ve bu da tek tek jetonların değerini aşındırabilir. Özellikle, az bulunan NFT'lerin değeri, artan nadirlikleri ve talepleriyle birlikte yükselir. Nadirliğe yapılan bu vurgu, değerli sanat eserleri gibi kültürel veya tarihi değere sahip NFT'ler için özel bir öneme sahiptir.

Güvenli Blockchain İşlemleri: NFT'lerin Veri Bütünlüğünün Sağlanması

NFT'ler blockchain teknolojisi ile hayatımıza girmiş kripto varlıklardır. Benzersiz dijital verilerdir, bu nedenle "değiştirilemez" olarak tanımlanırlar. NFT'lerin tıpkı DNA gibi benzersiz bir dijital imzası vardır. Sanat eserlerinin ilgili platforma kaydedilmesi ve web 3.0 tabanlı metaverse (oyun ekosistemlerinde dijital varlıkların oluşturulması) NFT'lerin kullanım alanlarına örnek olarak verilebilir.

Güvenli Blockchain İşlemleri: NFT'lerin Güvenli Saklanması

NFT'lerin güvenli bir şekilde saklanması için çeşitli yöntemler vardır. NFT'leri saklamanın en yaygın yolu, Blockchaindeki benzersiz kimlikleri kullanarak NFT'lerin sahipliğini ve gerçekliğini garanti eden bir cüzdan kullanmaktır. Bu cüzdanlar, NFT'lerin gerçekliğini ve sahipliğini korumak için özel olarak tasarlanmıştır. NFT'leri saklamak için bir başka yöntem de IPFS (InterPlanetary File System) adı verilen bir protokol kullanmaktır. IPFS dağıtılmış, merkezi olmayan ve eşler arası (P2P) bir depolama ağına dayanmaktadır.

Ağ, yüklenen dosyaları birden fazla bilgisayarda depolar. Böylece IPFS daha güvenli bir veri depolama deneyimi sağlar.

NFT'lerin Maruz Kalabileceği Kimlik Avı Saldırıları

Kimlik avı, insanları bir banka veya tanınmış bir şirket gibi meşru bir kuruluşla etkileşime girdiklerine inandırır. Bu genellikle meşru bir kurumdan geliyormuş gibi görünen bir e-posta veya kısa mesaj yoluyla yapılır. Alıcıdan mesajda şifre veya kredi kartı numarası gibi hassas bilgileri vermesi istenir.

Kimlik avı saldırısı genellikle e-posta yoluyla yapılır. Kurban, tanıdık gelebilecek bir web sitesi sayfasına giriş yapmasını isteyen bir e-posta alır. Ancak, web sitesi saldırı için taklit edilir ve kurban oturum açtığında kimlik bilgileri kötü niyetli aktörlere ifşa edilir.

Kimlik avı saldırıları kripto varlıklarını ele geçirmek ya da başka bir deyişle çalmak için de kullanılır. Örneğin, kötü niyetli bir kişi sahte bir web sitesi kopyası oluşturabilir. Bu şekilde, tüccar tarafından sağlanan cüzdan adresini kendi cüzdanı ile değiştirebilir ve kurbanı bir hizmet için ödeme yapmaya ikna edebilir.

Kimlik avı saldırılarına karşı korunmak için dolandırıcılık türlerini bilmek çok önemlidir. Çünkü bazı siber saldırılar ya da dolandırıcılık işlemleri karmaşık bir yapıya sahiptir ve mağdur için çok pahalıya mal olabilir. Bir kişinin oltalama saldırısından şüphelendiği ve hissettiği durumlarda bazı işaretleri görmesi gerekir. Bir oltalama saldırısının kendini ele verebileceği en yaygın belirtiler aşağıdaki gibidir:

- Acil, şimdi, hemen vb. ifadelerin sıkça kullanıldığı mesajlar
- Kişisel ve ticari bilgi talepleri içeren içerikler
- Kısaltılmış URL'ler içeren ve kişiyi web sitelerine yönlendiren metinler genellikle kimlik avı için kullanılır.

Bu Saldırılara Karşı Alınabilecek Önlemler

Örneğin, kimlik avı saldırılarının nasıl gerçekleştiğini ve bunların nasıl fark edileceğini öğrenmek çok önemlidir. Kimlik avı saldırıları genellikle e-posta yoluyla gerçekleşir. Bu nedenle, e-postalarınızı dikkatle kontrol etmeniz ve şüpheli bir e-posta aldığınızda açmamanız çok önemlidir. Ayrıca e-postaların gönderen adresini kontrol etmeli ve şüpheli bir adres görürseniz silmelisiniz. Kimlik avı saldırılarına karşı korunmak için güçlü bir şifre kullanmak ve düzenli olarak değiştirmek de çok önemlidir. İki faktörlü kimlik doğrulama gibi ek güvenlik önlemleri de alabilirsiniz. Bu, hesabınızın güvenliğini artırır. İki faktörlü kimlik doğrulama, kullanıcıların hesaplarına erişmek için yalnızca bir parola kullanması yerine, parola ve doğrulama kodu gibi iki farklı bileşenin kullanılmasını gerektirir. Böylece hesaplar daha güvenli hale gelir.

Güvenli Blockchain İşlemleri: Kripto Para Cüzdanları

Kripto para cüzdanları, kripto paraları güvenli bir şekilde saklamak için özel araçlar olarak hizmet eder. Tipik olarak donanım, yazılım veya kağıt cüzdan olarak mevcut olan bu araçlar, dijital varlıkların korunması için çeşitli seçenekler sunar. Kripto para cüzdanlarının güvenliği, özellikle değerlerinin artmasıyla birlikte daha da kritik hale gelmiştir. Güvenilir kripto para cüzdanlarına örnek olarak aşağıdakiler verilebilir:

Binance Wallet

Ledger

Coinbase

TrustWallet

MetaMask

Crypto.com

Bu cüzdanlar kripto para birimlerini güvenli bir şekilde saklamak için tasarlanmıştır. Her cüzdanın avantajları ve dezavantajları vardır. Bu nedenle kullanıcılar ihtiyaç ve tercihlerine göre en uygun kripto para cüzdanını seçmelidir.

Akıllı Sözleşmeler

Blok zinciri üzerinde çalışan otomatik ve koşullu kod parçalarına akıllı sözleşmeler denir. Bu akıllı sözleşmelerin güvenlik unsurları kod kalitesi, doğrulama mekanizmaları, hata işleme ve güncelleme kabiliyeti gibi faktörlere bağlıdır.

Güvenli Blockchain İşlemleri: Dijital varlıklarınızı ve kimliğinizi korumak için en iyi uygulamalar

Güçlü ve benzersiz parolalar kullanmak

Hesaplarınızın güvenliğini sağlamak için güçlü ve benzersiz parolalar kullanmak önemlidir. Güçlü bir parola, tahmin edilmesi ve kırılması zor olan bir paroladır. Benzersiz bir parola, diğer hesaplarınızda kullandığınız parolalardan farklıdır. İşte güçlü ve benzersiz bir parola oluşturmak için bazı ipuçları:

- Parolanız en az 12 karakter uzunluğunda olsun.
- Büyük harfler, küçük harfler, rakamlar ve semboller kullanın.
- Kişisel bilgileri veya hızlı tahmin edilebilir bilgileri kullanmaktan kaçının.
- Şifrenizi düzenli olarak değiştirin.
- Her hesap için farklı bir parola kullanın.

Sağlam ve benzersiz bir parola oluşturmak için, örneğin bir şarkı sözünden veya şiirden bir mısra veya anlamlı bir alıntı kullanabilirsiniz. Parolanızı güçlendirmek için bazı harfleri rakamlara veya sembollere

dönüştürebilirsiniz. Örneğin, “Futbol oynamayı seviyorum” cümlesinden “1L0v3t0Pl@yS0cc3r” gibi bir şifre oluşturabilirsiniz.

Parolanızı unutmamak için bir parola yöneticisi kullanabilirsiniz. Parola yöneticileri güçlü ve benzersiz parolalar oluşturmanıza ve tüm hesaplarınız için farklı parolalar saklamanıza yardımcı olur. Böylece her hesap için ayrı ve güvenli bir parola kullanabilirsiniz.

İki Aşamalı Kimlik Doğrulamayı Etkinleştirme

İki faktörlü kimlik doğrulama, hesaplarınızı güvence altına almak için kullanabileceğiniz bir yöntemdir. Bu İki faktörlü kimlik doğrulama, hesabınıza erişmek için birlikte çalışan iki farklı bileşenin kullanılmasını içerir.

Söz konusu bu güvenlik önlemi, hesabınıza yalnızca sizin erişebilmenizi sağlamayı amaçlamaktadır.

Güncel Bir Antivirüs Programı Kullanmak

Güncel bir antivirüs programı kullanmak bilgisayarınızı kötü amaçlı yazılımlardan korumak için çok önemlidir. Bu programlar sisteminizdeki kötü amaçlı yazılımları özenle tespit eder ve ortadan kaldırır. Kötü amaçlı yazılımların bilgisayarınızın performansını düşürebileceği, veri bütünlüğünü tehlikeye atabileceği ve hırsızlığı kolaylaştırabileceği göz önüne alındığında, güncel bir antivirüs programına sahip olmak sisteminizi güncel tehditlere karşı korur ve kötü amaçlı yazılım bulaşmalarını önler. Dahası, antivirüs yazılımı tehlikeli web sitelerini etkili bir şekilde engeller ve e-posta eklerini kapsamlı bir şekilde tarar. Bunu yapmak, bilgisayarınızın savunmasını kötü amaçlı yazılımlara karşı etkili bir şekilde güçlendirebilir. Antivirüs programlarını düzenli olarak güncellemek de aynı derecede hayati önem taşır. Bu güncellemeler, antivirüs yazılımının yeni ortaya çıkan tehditlere karşı korumasını güçlendirir ve böylece bilgisayarınızın genel güvenliğini artırır.

Güvenilir Kaynaklardan İndirilen Uygulamaları Kullanmak

Bilgisayarınızı kötü amaçlı yazılımlardan korumak için güvenilir kaynaklardan indirilen uygulamaları kullanmak önemlidir. Kötü amaçlı yazılımlar bilgisayarınızın performansını düşürebilir ve verilerinizi çalabilir ya da zarar verebilir. Güvenilir kaynaklardan indirilen uygulamalar genellikle resmi uygulama mağazalarında bulunur. Örneğin, Android cihazlar için Google Play Store ve iOS cihazlar için App Store ücretli uygulama mağazalarıdır. Bu mağazalardan uygulamalar indirilebilir ve güvenle kullanılabilir. Güvenilmeyen kaynaklardan indirilen uygulamalar bilgisayarınıza zarar verebilir veya kötü amaçlı yazılım içerebilir. Bu nedenle, uygulamaları yalnızca güvenilir kaynaklardan indirmeniz önerilir.

Kişisel Bilgilerinizi Sosyal Medyada Paylaşmamak ve Kimlik Avı E-postalarına Tıklamamak

Sosyal medyada kişisel bilgilerinizi paylaşmamanız ve kimlik avı e-postalarına tıklamamanız için birçok önemli neden vardır. Siber korsanlar, siber zorbalar, siber takipçiler, kimlik avcıları ve diğer kötü niyetli kişiler sosyal medyada paylaştığınız bilgileri manipüle edebilir. Bu istismarın potansiyel sonuçları sizin için ciddi sonuçlar doğurabilir. Örneğin;

Kimlik hırsızlığı: Sosyal medyada paylaştığınız bilgiler kimliğinizi çalmak ve sahte hesaplar açmak için kullanılabilir. Bu durum maddi kayıplara, itibarınızın zedelenmesine ve yasal sorunlara yol açabilir.

Doxxing(kişisel bilgileri toplama)

Sosyal medyada paylaştığınız bilgiler adresiniz, telefon numaranız veya iş yeriniz gibi hassas bilgiler içerebilir.

Sizi taciz veya tehdit etmek isteyen kişiler bu bilgileri çevrimiçi olarak paylaşabilir. Bu durum ruhsal sıkıntıya, güvenlik risklerine ve kariyer sonuçlarına neden olabilir.

Siber Zorbalık ve Taciz

Sosyal medyada paylaştığınız bilgiler, görüşleriniz, tercihleriniz veya yaşam tarzınız gibi kişisel yönlerinizi ortaya çıkarabilir. Sizi eleştirmek isteyen kişiler bu bilgileri sizi aşağılamak veya taciz etmek için kullanabilir. Bu durum öz saygınızı, ruh halinizi ve sosyal ilişkilerinizi olumsuz etkileyebilir.

Siber Takip

Sizi takip etmek veya gözetlemek isteyen kişiler sosyal medyada paylaştığınız bilgileri kullanarak konumunuzu, faaliyetlerinizi ve arkadaşlarınızı ifşa edebilir. Sonuç olarak, bu saldırı gizliliğinizi ihlal edebilir ve fiziksel güvenliğinizi riske atabilir.

Manipülatif Reklamcılık

Sosyal medyada bilgi paylaşmak ilgi alanlarınızı, alışkanlıklarınızı veya tercihlerinizi ortaya çıkarabilir ve daha sonra size özel reklamların sunulmasını sağlayabilir. Sonuç olarak, bu reklamlar karar verme sürecinizi etkileyebilir ve sizi istenmeyen veya gereksiz satın alımlara yönlendirebilir.

Kimlik Avı Saldırıları

Sosyal medyada paylaşılan bilgiler, şifreler veya kredi kartı numaraları gibi hassas bilgileri ifşa etmeniz için sizi kandırmak amacıyla istismar edilebilir. Bu saldırılar genellikle gerçek kuruluşları taklit eden e-postalar veya mesajlar yoluyla gerçekleşir. Bu tür saldırılara maruz kalmak, hesapların ele geçirilmesine veya finansal dolandırıcılığa maruz kalmanıza neden olabilir.

Kariyere İlişkin Sonuçlar

Sosyal medyada paylaştığınız bilgiler işverenleriniz veya potansiyel işverenleriniz tarafından görülebilir. Bu bilgiler profesyonel imajınızı veya uygunluğunuzu etkileyebilir. Örneğin, işe alım sırasında sosyal medya profilleriniz incelenebilir ve uygunsuz içerik nedeniyle reddedilebilirsiniz. Ayrıca mevcut işvereniniz hakkında olumsuz yorumlarda bulunmanız işten çıkarılmanıza da yol açabilir.

Bu nedenlerle, sosyal medyada paylaştığınız bilgileri sınırlandırmak ve gizlilik ayarlarınızı kontrol etmek çok önemlidir. Ayrıca paylaştığınız bilgilerin kaynağını ve doğruluğunu da kontrol etmelisiniz. Sosyal medyada paylaştığınız bilgiler sizin için birçok fayda sağlayabilir, ancak aynı zamanda birçok risk de taşıyabilir. Bu nedenle, sosyal medyayı akıllıca ve sorumlu bir şekilde kullanmanızı tavsiye ederiz.

Kimlik Avı E-postalarına veya Mesajlarına Tıklamamak

Kimlik avı e-postalarına veya mesajlarına tıklamamak bilgisayarınızı ve kişisel bilgilerinizi korumak için çok önemlidir. Sahte Kimlik avı, siber korsanların sahte e-postalar veya mektuplar göndererek sizden hassas veriler istediği bir saldırı yöntemidir. Bu veriler arasında şifreniz, kredi kartı numaranız, banka hesabınız veya kimlik bilgileriniz yer alır. Kimlik avı e-postaları veya mesajları genellikle meşru kuruluşları taklit eder ve sizden acil bir işlem yapmanızı veya bir bağlantıya tıklamanızı ister. Bu bağlantılar sizi sahte bir web sitesine yönlendirir ve bilgilerinizi girmenizi ister. Böylelikle siber korsanlar bilgilerinizi ele geçirir ve kötü amaçlar için kullanabilir.

Dijital Cüzdanınızın Yedeklemesini Yapmak

Dijital cüzdanınızın bir yedeği sizi bilgisayar arızalarına ve birçok insan hatasına karşı koruyabilir. Ayrıca, cüzdanınız şifrelenmişse, cep telefonunuz veya bilgisayarınız çalındıktan sonra bile kurtarabilirsiniz. Kimi cüzdanlar dahili olarak çok sayıda gizli özel anahtar kullanır, bu nedenle tüm cüzdanınızı yedeklemeniz önemlidir.

Co-funded by
the European Union

Dijital Varlıklarınızı Soğuk Cüzdanlarda Saklamak

Soğuk cüzdanların internete bağlı sıcak cüzdanlardan daha güvenli olduğu düşünülmektedir. Soğuk cüzdanlar genellikle USB sürücü gibi görünebilen donanım aygıtlarıdır.

Sıcak cüzdanlar bilgisayarınız veya telefonunuz aracılığıyla internete bağlanırken, soğuk cüzdanlar verilerinizi çevrimdışı tutmak için donanım aygıtları kullanır. Sıcak cüzdanlar alım satım için erişimi kolaylaştırırken, soğuk cüzdanlar uzun süreli depolama için daha uygundur. Her iki tür de genellikle kripto anahtarlarınızı korur – şifreleme ile oluşturulan harf ve sayı dizileri kripto işlemlerinizi yetkilendirebilir. Doğru cüzdan türü, ne kadar kripto tuttuğunuza, güvenlik tercihlerinize ve fonlarınıza ne kadar kolay erişmeniz gerektiğine bağlıdır.

Güvenli Blockchain İşlemleri: Sonuç

“Güvenli Blockchain İşlemleri” başlıklı bu makalede, dijital varlıklarınızı korumanın ve blockchain işlemlerinizi güvence altına almanın önemi vurgulandı. Mülkiyet haklarınızı korumak, veri bütünlüğünü sağlamak ve siber tehditlere karşı savunmak için anahtar kelime odaklı “Güvenli Blockchain İşlemleri” stratejilerini inceledik. Bu stratejiler, dijital yatırımcılar ve blok zinciri teknolojisi meraklıları için güçlü bir temel oluşturmayı amaçlıyor. Unutmayın, güvenli NFT’ler ve blok zinciri işlemleri geleceğe daha sağlam ve güvenli bir adım atmamıza yardımcı olacaktır.

Teşekkürler!

Co-funded by
the European Union

Akıllı Sözleşme Güvenliği: Riskleri Anlamak ve Azaltmak

Akıllı Sözleşme Güvenliği makalemize hoş geldiniz! Bu blog yazısını AB tarafından finanse edilen "V2B: Sanat Mesleki Eğitim Kursiyerleri için Metaverse üzerinde NFT Fırsatları Yaratmak" projesi için oluşturduk ve proje referans numaramız 2022-1-DE02-KA210-VET-000080828. L4Y Learning for Youth GmbH tarafından koordine edilen ve Adana Çukurova Güzel Sanatlar Lisesi ve EMC Services Ltd. işbirliğiyle hazırlanan "Dijital Varlık Güvenliği Stratejileri" başlıklı eğitimin çerçevesi giriş yazısında yer almaktadır.

Akıllı sözleşmeler, dijital çağda anlaşmaların yürütülme ve işlemlerin gerçekleştirilme biçiminde bir devrim yarattı. Blockchain teknolojisinin ve uygulamalarının karmaşık dünyasına girdikçe, akıllı sözleşme güvenliği kavramını anlamak çok önemli hale geliyor. Önceden tanımlanmış koşullarla kodlanmış, kendi kendini yürüten bu sözleşmeler benzersiz bir şeffaflık ve verimlilik sunarken, aynı zamanda yeni bir zorluklar ve güvenlik açıkları alanını da beraberinde getirmektedir. Bu makalede, akıllı sözleşme güvenliğinin çok yönlü ortamını keşfedecek, ilgili riskleri, bu sözleşmeleri korumak için tasarım ilkelerini ve potansiyel tehditleri azaltmak için mevcut araç cephaneliğini inceleyeceğiz. Merkeziyetsiz geleceğimize güç veren dijital anlaşmaları güvence altına almanın karmaşıklığını çözerken bu yolculukta bize katılın.

Öğrenme Hedefleri

Bu modülün sonunda, öğrenciler şunları yapabilecektir:

Akıllı sözleşmenin ne olduğunu ve tarihsel geçmişini tanımlayabilecektir.

Sözleşmelerin tarihsel gelişimini ve farklı dönemlerdeki önemini tanımlayabilecektir.

Bir sözleşmeyi geçerli kılan temel unsurları açıklayabilecektir.

Blockchain teknolojisinde akıllı sözleşmelerin özelliklerini ve avantajlarını listeleyebileceklerdir.

Akıllı sözleşmeler için temel güvenlik hususlarını tanımlayabilecektir.

Bu Akıllı sözleşmelerin güvenliğinde tasarım ilkelerinin rolünü anlayabilecektir.

Akıllı sözleşme geliştirmeye yönelik güvenilir platformları ve bunların benzersiz özelliklerini tanıyabileceklerdir.

Sözleşme Nedir ve Tarihsel Gelişimi Nasıl Olmuştur?

Sözleşme, bir anlaşmanın şartlarını ortaya koyan ve bir anlaşmaya vardıklarında tarafların hak ve yükümlülüklerini tanımlayan bir belgedir. Sözleşmelerin tarihi insanlık tarihi kadar eskidir. İlk sözleşmeler insanlar mallarını değiş tokuş ederken yapılmıştır. İlk yazılı sözleşmenin M.Ö. 2100 yılında yapıldığı bilinmektedir.

İnsanların ihtiyaçları ve sosyal yapıdaki değişimler sözleşmelerin gelişimini şekillendirmiştir. Örneğin, Roma hukukunda sözleşmeler öncelikle borç ilişkilerini düzenlemeye hizmet etmiştir. Orta Çağ boyunca sözleşmeler, toprak sahipleri ve köylüler arasındaki ilişkilerin düzenlenmesinde ağırlıklı olarak kullanılmış, Sanayi Devrimi'nden sonra ise sözleşmeler işçi hakları ve işverenlerin sorumlulukları gibi konuları da kapsamaya başlamıştır.

Günümüzde sözleşmeler hemen hemen her alanda kullanım alanı bulmaktadır. Örneğin, istihdam, kiralama, sigorta ve lisanslama gibi çeşitli alanlarda iş sözleşmeleri, kira sözleşmeleri, sigorta sözleşmeleri ve lisans sözleşmeleri gibi sözleşmeler yaygın olarak kullanılmaktadır.

Sözleşmelerin güvenliği çok önemlidir çünkü bu belgelerdeki hatalar ciddi mali kayıplara neden olabilir. Bu nedenle sözleşme hazırlama sürecinde dikkatli olmak gerekir.

Sözleşmenin Unsurları

Bir sözleşmenin unsurları, bir sözleşmenin geçerli sayılabilmesi için bulunması gereken unsurlardır. Bir sözleşmenin unsurları aşağıdaki gibidir:

-Taraflar: Sözleşme en az iki taraf arasında akdedilir.

- Konu: Sözleşmenin konusu belirli bir şey veya hizmet olmalıdır.
- Karşılıklılık: Sözleşmede taraflar arasında karşılıklı hak ve yükümlülükler bulunmalıdır.
- Hukuka uygunluk: Sözleşme hukuka uygun olmalıdır.
- Gönüllülük: Taraflar sözleşmeyi kendi iradeleri ile yapmış olmalıdır.

Sözleşmenin unsurları, sözleşmenin geçerli sayılabilmesi için bulunması gereken bileşenlerdir. Bu unsurların tamamı sağlandığında sözleşme geçerli kabul edilir.

Akıllı Sözleşme Nedir? Ne Zaman ve Neden Ortaya Çıktı?

Akıllı sözleşme, bir blok zinciri ağı üzerinde çalışan ve taraflar bir anlaşmaya vardığında ve bu anlaşmanın şartlarını yerine getirdiğinde otomatik olarak yürütülen bir yazılım programıdır. Akıllı sözleşmelerin geçmişi 1990'ların başına kadar uzanmaktadır. İlk akıllı sözleşme avukat ve kriptolog Nick Szabo tarafından geliştirilmiştir. Szabo, banka veya hukuk sistemi gibi üçüncü taraf bir aracı olmadan bir sözleşmenin şartlarını uygulamak ve yerine getirmek için dijital bir sistem oluşturmakla ilgileniyordu.

Akıllı sözleşmeler, bir anlaşmanın blok zincirlerine gömülü sözleşme şartlarını otomatik olarak uygulayarak güvenilir bir üçüncü tarafın müdahalesine olan ihtiyacı ortadan kaldırır. Bitcoin ilk kripto para birimidir ve bu nedenle basit bir akıllı sözleşmenin ilk örneğidir. Ancak yapısı nedeniyle bitcoin yalnızca para transferi amacıyla kullanılmaktadır. Ethereum akıllı sözleşmeleri bu noktada Bitcoin'den ayrılır. Ethereum, blok zinciri üzerinde farklı bir algoritmik yol izleyerek birçok amaca hizmet edebilen akıllı sözleşmelerin geliştirilmesinde öncü olmuştur.

Akıllı Sözleşme Güvenliği: Özellikler ve Avantajlar

Bir blok zinciri ağı üzerinde çalışan akıllı sözleşmeler, taraflar anlaştığında ve sözleşme şartlarını yerine getirdiğinde otomatik olarak çalışan yazılım programlarıdır.

Taraflar arasındaki güven sorunlarını ele alan bu sözleşmeler önemli bir endişeyi ortadan kaldırır.

Kullanıcılara tam kontrol sağlayan akıllı sözleşmeler, aracılara veya kişilere olan gereksinimi ortadan kaldırır.

Bu sözleşmeler, merkezi otoritelerden, yasal sistemlerden veya harici yaptırım mekanizmalarından yoksun olarak bağımsız bir şekilde çalışır.

Akıllı sözleşmeler blok zinciri teknolojisini kullanarak çalıştıkları için yasal düzenlemelerde bazı farklılıklar gösterirler.

Yazılım algoritmaları akıllı sözleşmeleri şifreleyerek güvenliklerini artırır ve dağıtılmış defterler bunları saklar.

Ayrıca, akıllı sözleşmeler kurumlar veya şirketler için işlem hızlarını artırır ve merkezi olmayan bir şekilde çalışır.

Akıllı sözleşmelerin hukuki statüsü klasik anlamda bildiğimiz sözleşmelerden farklıdır. Ancak sözleşme hukukuna uygun niteliklere de sahip olan akıllı sözleşmelerin hukuken de bir sözleşme ilişkisi olarak kabul edilmesi muhtemeldir.

Akıllı Sözleşme ‘lerin Güvenlik Unsurları

Akıllı sözleşmelerin güvenlik unsurları çok önemlidir ve yazılım geliştirme sürecinin her aşamasında göz önünde bulundurulmalıdır. Bu süreçte akıllı sözleşmenin tasarlanmasından, kodlanmasına, test edilmesine ve son olarak yayınlanmasına kadar birçok farklı adım bulunmaktadır. Akıllı sözleşmelerin güvenliği için dikkat edilmesi gereken bazı noktalar aşağıdaki gibidir:

-Akıllı sözleşme tasarlanırken olası tüm senaryoların hesaba katılması zorunludur.
-Kodlama aşamasına geçildiğinde, akıllı sözleşmenin güvenliğini sağlamak için en iyi uygulamalara bağlı kalmak şarttır.
-Test aşamasında, akıllı sözleşme tüm senaryolar altında test edilmelidir.
-Yayınlama aşaması yaklaştıkça, akıllı sözleşmenin güvenliğini korumak için gerekli her türlü önlemi almak çok önemli hale gelir.

Akıllı sözleşmelerin güvenliği çok önemlidir çünkü bu sözleşmelerdeki hatalar ciddi mali kayıplara neden olabilir. Örneğin, geçmişte akıllı sözleşmelerdeki hatalar nedeniyle milyonlarca dolarlık kayıplar yaşanmıştır.

Akıllı Sözleşme Tasarımında Kullanılan Güvenilir Platformlar ve Özellikleri

Akıllı sözleşmeler, bir iş düzeninde zaman, para ve personel tasarrufunun yanı sıra farklı alanlardaki iş yüklerini azaltarak, doğruluk ve kesinlik yani değişmezlik ilkesine dayanan programlama modelleridir.

Bir iş alanındaki prosedürleri, aracıları ve aksaklıkları ortadan kaldırmayı hedeflerler. Birçok platformda bu amaçla yazılmış ‘Akıllı Sözleşme’ modelleri oluşturabilirsiniz. Akıllı sözleşmeler üzerine Blockchain Danışmanlığı eğitiminde, akıllı sözleşme yazabileceğiniz platformlar hakkında bilgi edineceksiniz.

ERC20 Standartları

Ethereum tabanlı çalışmalarda ERC-20 temel alınır ERC-20 en güvenilir standartlardan biridir. Farklı ERC standartları olmasına rağmen Ethereum ERC-20 Standartlarını kullanmayı tercih etmiştir. Temel olarak ERC-20 kritic alanlarda kullanılması tavsiye edilmeyen ancak kullanıldığında size birçok farklı alanda birden fazla seçenek sunan bir Akıllı Sözleşme standart yapısına sahiptir.

Özellikler

- Kurulum ücretsizdir. Sözleşme işlemleri gaz olarak toplanır.

Ethereum'da "gas", ağ üzerinde belirli işlemlerin gerçekleştirilmesi için gereken hesaplama harcaması miktarını ölçen birimdir. Gaz fiyatı, her bir gaz birimi için ödemeyi kabul ettiğiniz eter miktarıdır. Gas fiyatını ve limitini ayarlayarak işleminizin ne kadar hızlı ve ne kadar maliyetli olacağını belirleyebilirsiniz.

- Ethereum Token standardı veya ERC-20 olarak kullanılır

Token, bir varlığı veya belirli bir kullanımı temsil eden ve blok zincirlerinde var olan bir kripto para türüdür. Geliştiriciler tokenları bağımsız blok zincirleri üzerine inşa etmek yerine mevcut blok zincirlerine entegre ederek oluşturur. Akıllı sözleşmeler adı verilen kodlar ve veritabanları ile çalışırlar. Yatırımcılar tokenları yatırım amacıyla, değer depolamak veya satın alma yapmak için kullanabilir.

- Kendi akıllı sözleşme programlama dili Solidity'yi kullanır
- Geliştiriciler için açık kılavuzlar mevcuttur
- Geliştirme topluluğu sürekli olarak güvenlik açıklarını araştırır
- Destek görüşmesi ortamı yaygındır / yardımcı olur
- Akıllı sözleşme geliştiricileri neredeyse her zaman Ethereum kullanarak deneyim sahibi olur ve geliştirirler.

Hyperledger Fabric

Ethereum'un rakipleri listesinde ilk sırada Hyperledger Fabric yer alıyor. Linux Vakfı, Aralık 2015'te başlayan Hyperledger projesini kurdu. Bu proje, blok zinciri tabanlı dağıtık defterlerin geliştirilmesini desteklemeyi amaçlayan açık kaynaklı bir projedir. IBM, öncelikle bir temel olarak kullandığı Hyperledger çerçevesi için güçlü bir desteğe sahiptir. IBM, Blockchain Çözümleri için akıllı sözleşmelere dayanan hemen hemen her iş modelinde Hyperledger'ı kullanıyor. Ciddi anlamda Hyperledger çalışmalarını desteklemekte ve bunların geliştirilmesinde öncü rol oynamaktadır.

Özellikler

- Açık Kaynak ve kullanımı ücretsiz
- Özel İzin üyelik sistemini destekler

Hyperledger Fabric, özel bir izin üyelik sistemi ile çalışan bir blockchain platformudur. Bu özelliği kullanarak, ağ erişimini yalnızca belirli kullanıcılarla kısıtlamak mümkün hale gelir. Bu kullanıcılar ağın diğer üyeleriyle etkileşime girebilir ve akıllı sözleşmeler yürütebilir.

Böylelikle geliştiriciler, yalnızca belirli kullanıcıların erişebileceği özel bir blok zinciri ağı oluşturabilir. Bu da işletmelerin özel bir blok zinciri ağı oluşturarak işlerini daha güvenli hale getirmelerine olanak tanıyor.

- IBM tarafından desteklenmektedir
- Sözleşmelerin çeşitli dillerde kodlanmasını sağlar
- Güvenilir performans
- Eklenti bileşenlerini destekler

"Eklenti", bir bilgisayar programına belirli bir özellik ekleyen küçük bir bilgisayar programıdır. Programlar eklentileri desteklediğinde, özelleştirmeye izin verirler. Örneğin, bir e-posta kutusunda hızlı arama yapmak ve kişilerle bağlantı kurmak için bir eklenti kullanabilirsiniz. Virüs taraması, dosya sıkıştırma ve dosya şifreleme yazılımlarını desteklemek için eklentiler kullanabilirsiniz.

Nem

Nem 31 Mart 2015 tarihinde piyasaya sürülmüştür. Java dünyada en yaygın kullanılan programlama dillerinden biri olduğu için bazı geliştiriciler tarafından tercih edilmektedir.

Bu, programcıların Solidity gibi platforma özgü programlama dillerini öğrenmelerine gerek kalmadığı için onu süper erişilebilir kılan bazı özelliklere sahiptir. Öne çıkan ikinci bir husus ise Java'nın çok daha gelişmiş olması ve bu nedenle Solidity gibi platforma özgü yeni dillere kıyasla daha az güvenlik açığına sahip olmasıdır.

Özellikler

- Java'da tasarım yapmak çok kolay
- Platforma özel programlama dili yok
- Ölçeklenebilirlik
- Mükemmel performans

Dezavantajları

- Diğer platformlara göre daha küçük geliştirme topluluğu
- Daha az araç mevcut
- Akıllı sözleşmeler yazmak için kullanılan bir programlama dili olan Solidity yerine kendi kodlama dili olan Mijin'i kullanır. Bu nedenle, merkeziyetsizliği Solidity kullanan diğer akıllı sözleşme platformları kadar güçlü değildir.

Stellar

2014 yılında kurulan Stellar, bu listedeki en eski akıllı sözleşme platformu olma özelliğine sahiptir. Stellar Development Foundation, Stellar'ı yönetiyor ve sürekli olarak en umut verici blok zinciri girişimlerinden biri olarak tanınıyor.

Stellar, mevcut altyapısının Ripple gibi sistemlere benzediği konusunda güçlü şirketleri ikna etmeyi ve mikro ödemeler ağı konusunda güçlü şirketleri ikna etmeyi başarmıştır. Bu nedenle Stellar, çalışma prensipleri doğrultusunda yoğun bir iletişim ağına ve farklı deneyimlere sahiptir.

Akıllı sözleşmeler için en iyi platform söz konusu olduğunda, Stellar Ethereum'dan daha basit ve kullanımı daha kolaydır, ancak belki Nem kadar kolay değildir. Bununla birlikte, tasarımı ICO'lar gibi basit akıllı sözleşmeleri başarıyla kolaylaştırır.

ICO, İngilizce "Initial Coin Offering" teriminin kısaltmasıdır ve kripto para birimi teklifi anlamına gelir. Projeler için fon toplamak amacıyla Bitcoin ve Ethereum gibi popüler kripto para birimleri karşılığında yeni üretilen bir token ya da kripto varlığın satışa sunulması sürecini tanımlar. ICO'lar, yeni bir token, coin, uygulama veya hizmet oluşturmak için para toplamak isteyen bir şirket tarafından başlatılan bir fon toplama yöntemi olarak tanımlanıyor. ICO ile yatırımcılar, projenin yerel kripto birimini piyasaya çıkmadan önce daha ucuza satın alabilirler.

Günümüzde ICO'ların çoğunu genellikle bir aracı kuruluş yürütmektedir.

- ICO'lar için ideal
- Ethereum'a kıyasla çok ucuz
- Basit bir platform
- İyi performans
- Sektörde saygı duyulan

Dezavantajları

Daha karmaşık akıllı sözleşme geliştirme için uygun değildir, ancak geliştirme çabaları devam etmektedir.

Diğer akıllı sözleşme platformları arasında EOS, Corda ve Ripple bulunmaktadır.

EOS

EOS.IO en temel haliyle bir akıllı sözleşme platformudur. Yani bir dapp üretmemizi sağlayacak bir platformdur.

DAPP, merkezi olmayan uygulamalar anlamına gelen Distributed Application'ın kısaltmasıdır. DAPP'ler merkezi bir otoriteye ihtiyaç duymadan çalışabilen uygulamalardır. Geliştiriciler bu uygulamaları blok zinciri teknolojisini kullanarak oluştururlar ve akıllı sözleşmeler aracılığıyla çalışırlar. DAPP'ler çok çeşitli alanlarda kullanım alanı bulabilir. Örnek vermek gerekirse, finansal hizmetler, oyun, sosyal medya ve diğer çeşitli sektörlerde uygulama bulabilirler. DAPP üretmek, bu uygulamaları geliştirmek anlamına gelir. DAPP üretmek için öncelikle bir blok zinciri platformu seçmeniz gerekir. Ethereum, EOS.IO ve TRON gibi platformlar DAPP geliştiricileri arasında oldukça popüler. Ardından, akıllı sözleşmeler oluşturmanız gerekir. Akıllı sözleşmeler, DAPP'lerin çalışmasını sağlayan kodlardır. Akıllı sözleşmeler oluşturmak için Solidity gibi bir programlama dili kullanabilirsiniz. Son olarak, DAPP'leri test etmeniz ve yayınlamanız gerekir. Bu noktada, DAPP'leri test etmek amacıyla bir test ağı kullanmanız tavsiye edilir.

Blockchain teknolojisi olan EOS'un üzerine inşa edilecek pek çok farklı uygulama var, çünkü bu teknolojinin gerçekten neler yapabileceğini henüz keşfetmedik.

Özellikler

- Yüksek performans: EOS, yüksek hızlı işlem yapabilen bir blok zinciri platformudur.
- Ölçeklenebilirlik: EOS ölçeklenebilirlik sorunlarını çözmeyi amaçlamaktadır.
- Delegasyon: EOS bir delegasyon sistemi kullanır.

EOS bir delegasyon sistemi kullanır. Bu sistemde, EOS sahipleri gibi paydaşlar delegeleri seçmek için oy kullanır. Seçilen bu delegeler blok üretme yetkisi kazanır. Bu tasarım blok zinciri güvenliğini artırmayı amaçlamaktadır. Delegasyon sistemi blok zincirindeki işlemleri doğrular ve bloklar oluşturur. Bu şekilde blok zinciri daha hızlı ve daha güvenli hale gelir. Dahası, delegasyon sistemi blok zinciri içindeki işlemlerin doğruluğunu sağlayarak onu daha güvenli hale getirir.

- İşlem ücretleri: EOS, işlem ücretlerinin kullanıcılar tarafından ödenmediği, ancak blok üreticileri tarafından karşılandığı bir sistem kullanır.
- Esneklik: EOS farklı programlama dillerini desteklemektedir.
- Düşük gecikme süresi: İyi bir kullanıcı deneyimi, birkaç saniyeden fazla olmayan bir gecikme ile güvenilir geri bildirim gerektirir. Daha uzun gecikme süreleri kullanıcıları hayal kırıklığına uğratır ve blok zinciri olmayan uygulamaları mevcut blok zinciri olmayan alternatiflerle daha az rekabetçi hale getirir. Platform, işlemlerin düşük gecikme sürelerini desteklemelidir.
- Sıralı Performans: Bazı uygulamalar, sıralı olarak bağımlı adımları nedeniyle paralel algoritmalar uygulayamaz. Borsa gibi uygulamalar yüksek hacimleri işlemek için yeterli sıralı performansa ihtiyaç duyar. Bu nedenle platform hızlı sıralı performansı desteklemelidir.
- Paralel performans: Büyük ölçekli uygulamaların iş yükünü birden fazla CPU ve bilgisayar arasında bölüştürmesi gerekir. Konsensüs Algoritması – Delegated Proof Of Stake (dPoS) EOS, dPoS konsensüs algoritmasını kullanır.
- Bu algoritma, paydaşların, özellikle de EOS sahiplerinin, delegeleri seçmek için oy kullanması ve bu seçilen delegelere blok üretme yetkisi vermesi anlamına gelir.

Özellikler

- Yüksek performans: EOS, yüksek hızlı işlem yapabilen bir blok zinciri platformudur.
- Ölçeklenebilirlik: EOS ölçeklenebilirlik sorunlarını çözmeyi amaçlamaktadır.
- Delegasyon: EOS bir delegasyon sistemi kullanır.

EOS bir delegasyon sistemi kullanır. Bu sistemde, EOS sahipleri gibi paydaşlar delegeleri seçmek için oy kullanır. Seçilen bu delegeler blok üretme yetkisi kazanır. Bu tasarım blok zinciri güvenliğini artırmayı amaçlamaktadır. Delegasyon sistemi blok zincirindeki işlemleri doğrular ve bloklar oluşturur. Bu şekilde blok zinciri daha hızlı ve daha güvenli hale gelir. Dahası, delegasyon sistemi blok zinciri içindeki işlemlerin doğruluğunu sağlayarak onu daha güvenli hale getirir.

- İşlem ücretleri: EOS, işlem ücretlerinin kullanıcılar tarafından ödenmediği, ancak blok üreticileri tarafından karşılandığı bir sistem kullanır.
- Esneklik: EOS farklı programlama dillerini desteklemektedir.

- Düşük gecikme süresi: İyi bir kullanıcı deneyimi, birkaç saniyeden fazla olmayan bir gecikme ile güvenilir geri bildirim gerektirir. Daha uzun gecikme süreleri kullanıcıları hayal kırıklığına uğratır ve blok zinciri olmayan uygulamaları mevcut blok zinciri olmayan alternatiflerle daha az rekabetçi hale getirir. Platform, işlemlerin düşük gecikme sürelerini desteklemelidir.
- Sıralı Performans: Bazı uygulamalar, sıralı olarak bağımlı adımları nedeniyle paralel algoritmalar uygulayamaz. Borsa gibi uygulamalar yüksek hacimleri işlemek için yeterli sıralı performansa ihtiyaç duyar. Bu nedenle platform hızlı sıralı performansı desteklemelidir.
- Paralel performans: Büyük ölçekli uygulamaların iş yükünü birden fazla CPU ve bilgisayar arasında bölüştürmesi gerekir. Konsensüs Algoritması – Delegated Proof Of Stake (dPoS) EOS, dPoS konsensüs algoritmasını kullanır.
- Bu algoritma, paydaşların, özellikle de EOS sahiplerinin, delegeleri seçmek için oy kullanması ve bu seçilen delegelere blok üretme yetkisi vermesi anlamına gelir.

Dezavantajları

- EOS.IO diğer blok zincirlerine kıyasla daha az popülerdir.
- Bazı kullanıcılar EOS.IO'nun merkeziyetsiz bir platform olmasına rağmen merkezi bir yapıya sahip olduğunu iddia etmektedir.

Corda

Corda, açık kaynaklı bir yazılım projesi olan Corda platformundan oluşmaktadır. Düzenlenmiş piyasalar için tasarlanmış önde gelen açık, izinli dağıtılmış uygulama platformudur. Corda platformu bir dizi standarttan, ağ parametrelerinden ve ilgili yönetişim süreçlerinden oluşur. Bu, açık ağdaki herhangi bir kuruluşun veya bireyin başka herhangi bir kuruluş veya bireyle doğrudan işlem yapmasına olanak tanır. Corda'nın temel özellikleri şunlardır:

- Ölçeklenebilirlik: Corda ölçeklenebilirlik sorunlarını çözmeyi amaçlamaktadır.
- Merkezi olmayan: Corda merkezi olmayan bir platformdur.
- Güvenli: Corda mevcut yasal yapılarla uyumludur ve ISO 20022 ve ISDA CDM gibi mevcut ve yeni çıkan düzenlemelerle uyumludur.
- Akıllı sözleşmeler: Corda akıllı sözleşmeler kullanarak çalışır.
- Modülerdir: Corda modüler bir geliştirme çerçevesidir. İhtiyacınız olan yetenekleri kullanmanıza olanak tanır.
- İşlem ücretleri: Corda, işlem ücretlerinin kullanıcılar tarafından ödenmediği, blok üreticileri tarafından karşılandığı bir sistem kullanır.
- Özel: Corda, tasarımcılar tarafından özel işlemler için uyarlanır.

Dezavantajları

- Diğer blok zincirleri CORDA'dan daha popülerdir.
- Bazı kullanıcılar CORDA'nın yeterli merkeziyetçilikten yoksun olduğunu iddia etmektedir.

Ripple

Blok zinciri teknolojisi üzerine inşa edilmiş bir kripto para birimi olarak duruyor. Ripple, finansal hizmetler endüstrisi için bir dizi çözüm sunmaktadır. Ripple'ın başlıca özellikleri aşağıdaki gibidir:

- Hızlı işlem: Ripple işlemleri hızlı bir şekilde işleyebilir.
- Düşük ücretler: İşlem ücretlerini düşük tutar.
- Ripple kullanılarak çevrimiçi ödeme kolaylaştırılabilir.
- Merkezi olmayan: Ripple merkezi olmayan bir platformdur.
- Yüksek güvenlik: Yüksek güvenlikli bir platformdur.
- Ölçeklenebilirlik: Ripple ölçeklenebilirlik sorunlarını çözmeyi amaçlamaktadır.

Dezavantajları

- Diğer blok zincirleri ondan daha fazla popülerliğe sahiptir.
- Bazı kullanıcılar yeterli merkeziyetsizliğe sahip olmadığını iddia etmektedir.

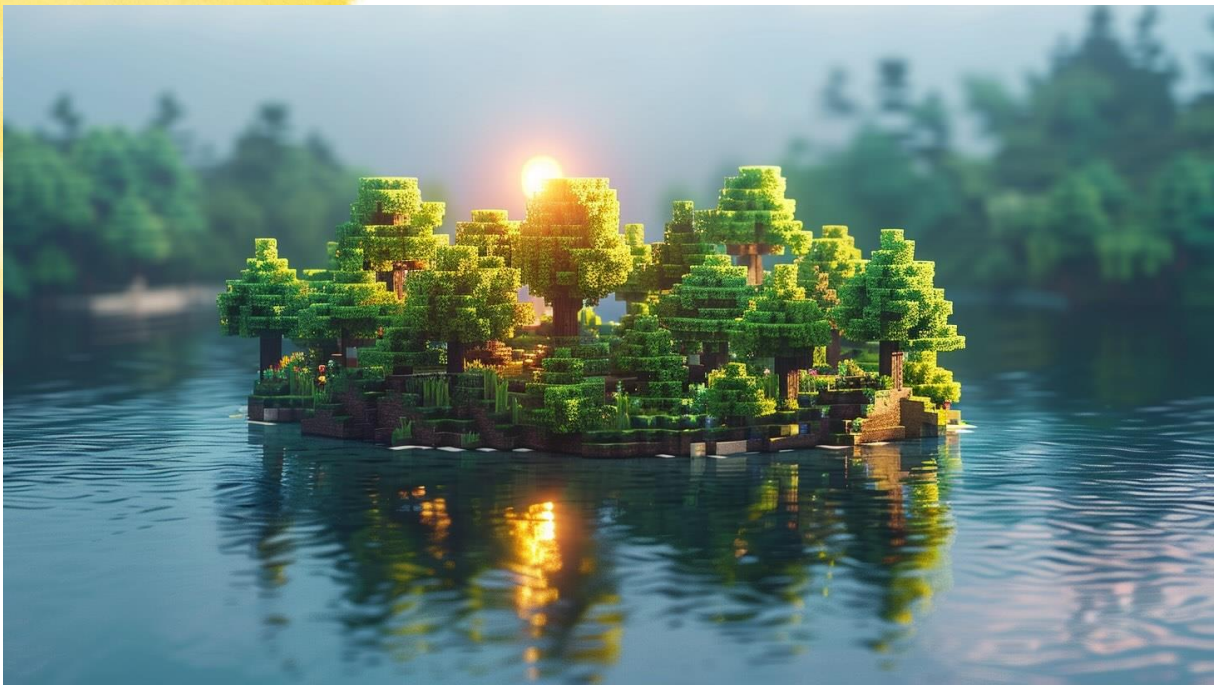
Co-funded by
the European Union

Akıllı Sözleşme Güvenliği: Sonuç

Akıllı sözleşmeler blok zinciri üzerinde bir uygulama türüdür. Blok zinciri üzerinde bir kurallar temeline sahip otomatik programlar olarak bulunurlar. Akıllı sözleşmeler şeffaflık, izlenebilirlik ve değişmezlik gibi avantajlar sunar. Ancak akıllı sözleşmeler bazı güvenlik riskleri de taşır. Bu riskler arasında hatalı kodlama, savunmasız kodlama, mantık hataları ve diğerleri yer alır. Akıllı sözleşmelerin güvenliği için bazı tasarım ilkeleri ve güvenlik önlemleri bulunmaktadır. Örneğin, uzmanlar akıllı sözleşmeler tasarlanırken modüler ve izole bir mimari kullanılmasını önermektedir. Ayrıca, hazır şablonlar kullanmak akıllı sözleşmelerin güvenliğini artırabilir. Akıllı sözleşmelerin güvenliği için birçok çerçeve ve araç da mevcuttur.
Bu araçlar, akıllı sözleşmelerin güvenliğini artırarak hataları tespit etmeyi ve saldırılara karşı savunmayı amaçlamaktadır.

Co-funded by
the European Union

Dijital Varlık Güvenliği Stratejileri



Bu blog yazısını AB tarafından finanse edilen “V2B: Sanat Mesleki Eğitim Kursiyerleri için Metaverse’de NFT Fırsatları Yaratmak” projesi için oluşturduk. Ve proje referans numaramız 2022-1-DE02-KA210-VET-000080828. L4Y Learning for Youth GmbH tarafından koordine edilen, Adana Çukurova Güzel Sanatlar Lisesi ve EMC Services Ltd. işbirliğiyle hazırlanan “Dijital Varlık Güvenliği Stratejileri” başlıklı eğitim çerçevesi ile ilgili olarak giriş yazısında yer verilmiştir.

Bu yazıda odak anahtar cümlemiz “Dijital Varlık Güvenliği Stratejileri” etrafında dönmektedir. Dijital kimlik kavramını, tarihsel bağlamını ve tanımlayıcı özelliklerini inceliyoruz. Ayrıca, dijital kimlik ve dijital varlıkların önemini kabul ediyoruz. Dahası, dijital varlıkları tanımlıyor, tarihçelerini ve benzersiz niteliklerini keşfediyoruz. Ayrıca dijital alandaki yaygın tehditleri ele alıyoruz. Öncelikli amacımız, bu varlıkları potansiyel risklere karşı korumaya yönelik öngörüler sunarak etkili önlemler ve stratejiler üzerinde durmaktır.

Dijital kimliklerimizi ve varlıklarımızı korumamız gerektiğini vurgulayarak, ne tür tehditlerle karşılaşabileceğimizi açıklayacağız. Sadece kimliğimizi ve varlıklarımızı kimlere karşı korumamız gerektiğini değil, aynı zamanda bunların hangi yöntemlerle gerçekleştirilebileceğini de tartışacağız. Özellikle blockchain teknolojisinin sunduğu avantajları ve potansiyel riskleri ele alacağız. Ayrıca, bu teknolojiyi kullanarak nasıl daha güvenli bir dijital varlık yönetimi sağlayabileceğimizi inceleyeceğiz.

Bu makalenin hedef kitlesi internet kullanan ve dijital varlık sahibi olan herkesi kapsamaktadır. Son olarak, amacımız okuyucularımızın dijital kimlik ve varlıklarının güvenliği konusunda farkındalık kazanmalarına yardımcı olmaktır. Ayrıca, bu konuda gerekli adımları atmalarını sağlamayı hedefliyoruz.

Öğrenme Hedefleri

Bu modülün sonunda, öğrenciler şunları yapabilmelidir:

- Dijital Kimliğin ne olduğunu tanımlama, tarihçesini ve özelliklerini açıklama
- “Dijital Varlık” terimini, tarihsel bağlamını ve temel özelliklerini tanımlayabilme
- Bir Dijital Kimlik oluşturmak için kullanılan temel özellikleri tanımlama
- Dijital Varlıklara ve Kimliğe yönelik başlıca tehdit türlerini listeleme ve tanımlama
- Blockchain varlıklarına özgü yaygın tehditleri belirleme
- Blockchain teknolojisinde varlıkları ve kimliği güvence altına almak için geliştirilebilecek koruma tekniklerini tanımlama

Co-funded by
the European Union

Dijital Kimlik Nedir? Tarihçesi ve Özellikleri Nedir?

Dijital kimlik, bir kişi veya kuruluşun dijital ortamda tanımlanmasını sağlar. Dijital kimlikler, insanların dijital dünyada kim olduklarını belirlemelerine yardımcı olan elektronik bir tanımlama sürecidir.

Bir dijital kimlik, bireyler veya kuruluşlar tarafından sahip olunan çeşitli kimlikleri içeren kapsamlı bir dijital temsili oluşturur. Günümüzün en moda kavramlarından biri olan dijital kimlik kavramı ile insanlar sıklıkla karşılaşmaktadır.

Dijitalleşmenin artmasıyla birlikte gerçek hayattaki kimliklerin de dijitale taşınmasına ihtiyaç duyuluyor. Dijital kimliklerin geçmişi 30 yıl öncesine dayanıyor. Modern internetin doğuşundan bu yana, yani 30 yıl öncesinden beri kullanılıyor. Ancak gerçek dünyadaki işlemlerin giderek dijitalleşmesiyle birlikte bunlara olan ilgi de arttı. Bu dijital kimlik kavramının henüz standart bir tanımı olmamasına rağmen, neredeyse tüm tanımlar aşağıdaki temel kavramlara dayanmaktadır:

Dijital Varlık Güvenliği Stratejileri: Dijital Kimlik tanımı

Dijital kimlik veya ID, bir bireyin çevrimiçi temsilini ve dokümantasyonunu ifade eder.

Benzersiz bir bireyle ilişkilendirilen her bir dijital kimlik, doğrulanmış ve saklanmış özniteliklerin bir koleksiyonudur.

Bu cümleyi daha akıcı ve net bir şekilde düzenleyebilirsiniz:

Dijital kimlikler, çevrimiçi hizmetlere erişim sağlarken kimlik doğrulama yapar. Ve dijital işlemler sırasında kimlik taleplerine yanıt verir.

Tıpkı gerçek dünyada olduğu gibi, dijital kimliklerin de bir dizi evrensel kuralı vardır:

Bir dijital kimlik kişisel olmalı ve devredilemez olmalıdır.

Erişim ve kullanım hakları sadece ait olduğu kişiye ait olmalıdır.

Dijital kimlik yeniden kullanılabiliyor olmalıdır. Kısacası, ihtiyaç duyulduğunda aynı dijital kimliği kullanmak mümkün olmalıdır.

Dijital kimliğin kullanımı herhangi bir teknik uzmanlık gerektirmeden her zaman erişilebilir olmalıdır.

Son olarak dijital kimlikler belirli eylemleri gerçekleştirmeli ve belirli hedefleri yerine getirmelidir.

Dijital Varlık Güvenliği Stratejileri: Dijital Kimlik Oluşturmak İçin Özelliklerin Belirlenmesi

İsim, doğum tarihi ve diğer kişisel bilgiler

Belirli çevrimiçi hizmetlere erişim için oturum açma kimlik bilgileri

E-posta adresleri

Pasaport numaraları

Sosyal Güvenlik numaraları

Tarayıcı hareketleri ve çevrimiçi arama faaliyetleri

Online alışveriş ve bununla ilgili faaliyetler

Co-funded by
the European Union

Dijital Varlık Güvenliği Stratejileri: Dijital Varlık Nedir? Tarihçesi ve Özellikleri Nedir?

Bir dijital varlık, bir kişinin veya kuruluşun dijital ortamda tanımlanabilir olmasını sağlayan bir kimlik türü olarak hizmet eder. Dijital varlıklar elektronik olarak oluşturulan, saklanan ve aktarılan ticari araçlardır. Dijital varlıkların geçmişi 30 yıl öncesine dayanmaktadır. Modern internetin doğuşundan bu yana, yani 30 yıldır kullanılmaktadır. Dijital varlıkların farklı sektörlerde kullanımı artmaya başlamıştır. Bu dijital varlıkların temel özellikleri aşağıdaki gibidir:

-Dijital varlıklar dijital formda mevcuttur ve fiziksel formda bir karşılığı yoktur.

-Üreticiler, fiziksel üretim ihtiyacını ortadan kaldırarak dijital varlıkları daha uygun maliyetle oluşturur ve kullanır.

-Dijital varlıklar hem merkezi olmayan hem de merkezi biçimlerde var olabilirler.

-Transferleri daha hızlıdır. Uluslararası transferleri de daha kolaydır.

Bu dijital varlıkların değerinin transferini yapabilirsiniz.

Dijital Varlık Güvenliği Stratejileri: Dijital Varlıklarımıza ve Kimliğimize Yönelik Olası Tehditler Nelerdir?

Dijital varlıklarınıza ve kimliğinize yönelik olası tehditler şunları içerir:

Kimlik Avı

Bu, bir saldırganın sahte bir web sitesi veya e-posta kullanarak kişisel bilgilerinizi çalmasını içerir.

Kimlik avı saldırıları, birisi sizi kişisel bilgilerinizi paylaşmanız için kandırmaya çalıştığında meydana gelir. Kimlik avcıları faaliyetlerini genellikle e-postalar, reklamlar veya halihazırda kullandığınız sitelere benzeyen siteler aracılığıyla yürütür. Örneğin, bankanızdan geliyormuş gibi görünen ve banka hesap numaranızı onaylamanızı isteyen bir e-posta alabilirsiniz. Kimlik avı sitelerinin isteyebileceği bilgiler arasında kullanıcı adları, şifreler, kimlik veya sigorta numaraları, banka hesap numaraları, PIN'ler (Kişisel Kimlik Numaraları), kredi kartı numaraları, annenizin kızlık soyadı ve doğum gününüz yer alır.

Dijital güvenlik için ciddi bir tehdit oluşturan kötü amaçlı yazılım, bir saldırgan tarafından bilgisayarınıza kötü amaçlı yazılım yüklenmesini gerektirir. Bu yazılım cihazınızda depolanan verilere yasadışı bir şekilde erişir. Ayrıca, sisteminizin kontrolünü ele geçirme riski de taşır. Kötü amaçlı yazılımların arkasındaki kötü niyetli niyetler çeşitli şekillerde ortaya çıkar. Veri hırsızlığı, cihaz manipülasyonu ve genel cihaz performansının bozulmasını kapsar. Kötü amaçlı yazılım alanında virüsler, solucanlar, Truva atları ve casus yazılımlar dahil olmak üzere çeşitli formlar mevcuttur. Bu formlardan biri olan virüsler, benzer bir çalışma yöntemini paylaşan solucanlar gibi kendi kendini çoğaltma yoluyla yayılırlar.

Toplum Mühendisliği

Bu, bir saldırganın sizi kişisel bilgilerinizi açıklamaya ikna etmek için manipüle etmesini içerir. Örneğin:

Bir saldırgan kendisini bankanın müşteri hizmetleri temsilcisi olarak tanıtarak sizi kişisel bilgilerinizi paylaşmaya ikna etmeye çalışır.

Öte yandan, bir saldırgan kendisini yakın bir arkadaşınız veya aile üyeniz olarak tanıtan bir e-posta göndererek sizden para talep eder.

Aldatıcı bir saldırgan meşru bir kuruluş gibi davranarak bir web sitesi oluşturarak kişisel bilgilerinizi veya kredi kartı bilgilerinizi paylaşmanız için sizi kandırır.

Şifre Kırma

Bu, bir saldırganın hesabınıza erişmek için şifrenizi kırmasını içerir.

Bu özel saldırı türünün örnekleri, her biri kendine özgü özelliklere sahip bir dizi kötü niyetli metodolojiyi kapsar. Kayda değer örnekler arasında kaba kuvvet saldırıları, parola püskürtme saldırıları, hash crack saldırıları ve gökkuşağı tablosu saldırıları yer alır. Kaba kuvvet saldırılarında, saldırganlar yetkisiz erişim elde etmek için sistematik olarak mümkün olan her parola kombinasyonunu dener. Benzer şekilde, parola püskürtme saldırıları yaygın olarak kullanılan, ortak parolaları kullanarak birden fazla hesabı denemeyi içerir. Hash crack saldırıları, gerçek şifreleri ortaya çıkarmak için şifrelerin hash değerlerini çözmeye odaklanır. Öte yandan, gökkuşağı tablosu saldırıları, önceden hesaplanmış bir karma değerler listesinden yararlanarak çalışmaktadır. Ve bu yöntemle parolanızı çıkarmaya çalışır. Bu örnekler, kötü niyetli aktörlerin dijital güvenliği tehlikeye atmak için kullandıkları çeşitli taktiklere ışık tutmaktadır.

Ağ Saldırıları

Bu, bir saldırganın doğrudan ağınıza veya cihazınıza saldırmasını içerir.

Ağ saldırıları, bilgisayar sistemleri, ağ altyapıları veya internete bağlı cihazlar üzerinde gerçekleştirilen kasıtlı ve zarar verici eylemleri içerir. Bu saldırıları bilgisayar korsanları, siber suçlular, devlet destekli aktörler veya kötü niyetli kişiler gibi çeşitli kişiler gerçekleştirebilirler.

Ağ saldırılarıyla, bilgi hırsızlığı, sistemin devre dışı bırakılması, veri manipülasyonu, hizmet kesintisi ve kullanıcı gizliliğinin ihlali gibi bir dizi zararlı sonuca yol açabilir. Bu ağ saldırılarının örnekleri aşağıdakileri kapsar:

DDoS (Dağıtılmış Hizmet Engelleme) Saldırıları: Birden fazla kaynaktan gelen trafiği hedef sisteme yönlendirerek ağ kaynaklarını tüketir. Ve böylece hizmet kesintisi yaratır.

Man-in-the-Middle (MitM) Saldırıları: İletişime dahil olan iki taraf arasına girerek verileri keser, manipüle eder ve izler.

ARP (Adres Çözümleme Protokolü) Zehirlenmesi Saldırıları: Ağdaki ARP tablosunu manipüle ederek hedef cihazın iletişimini keser ve yeniden yönlendirir.

Rogue AP (Sahte Erişim Noktası) Saldırıları: Yapay bir erişim noktası oluşturarak kullanıcıların ağ trafiğini yakalar ve manipüle eder.

VLAN Atlama Saldırıları: Sanal ağlarda VLAN trafiğini yetkisiz olarak geçirerek güvenlik duvarlarını atlatmayı amaçlar.

Botnet Saldırıları: Birçok bilgisayardan oluşan bir bot ağı ile hedef sistemlere saldırır ve kötü amaçlı işlemler gerçekleştirir.

Fiziksel Hırsızlık

Bu, bir saldırganın cihazlarınızı veya diğer dijital varlıklarınızı çalmasını içerir.

Dijital Varlık Güvenliği Stratejileri: Bu Tehditlere Karşı Geliştirilebilecek Savunma Teknikleri Nelerdir?

Dijital varlıklarınızı ve kimliğinizi hedef alabilecek tehditler ile bu tehditlere karşı geliştirebileceğiniz savunma teknikleri şunlardır:

Kimlik Avı

Bu, bir saldırganın sahte bir web sitesi veya e-posta kullanarak kişisel bilgilerinizi çalmasını içerir. Bu tür saldırılara karşı korunmak için, gelen e-postaları dikkatlice okuyun. Bilinmeyen kaynaklardan gelen bağlantılara tıklamayın. Ayrıca, güçlü parolalar kullanarak hesaplarınızı koruyun ve iki faktörlü kimlik doğrulama kullanın.

Güçlü parolalar oluşturarak başkalarının hesabınıza erişmesini engelleyebilirsiniz. Güçlü parolalar oluşturmanın en güvenli ve en kolay yolu Chrome'un sizin için parola önermesine izin vermektir. Kendi parolanızı oluşturmak istiyorsanız bu noktaları göz önünde bulundurun:

Dijital Varlık Güvenliği Stratejileri: Kendi Şifrenizi Oluşturmak İçin…

Her hesap için benzersiz bir parola kullanmak büyük önem taşır. Bu önlem çok önemlidir. Çünkü şifrelerin tekrar kullanılması önemli risklere yol açabilir. Yetkisiz kişiler, hesaplarınızdan yalnızca birinin şifresini ele geçirmesi durumunda, bu şifreyi kullanarak e-postanıza erişebilirler. Sosyal medya profillerinizin ve hatta finansal hesaplarınızın kontrolünü de ele geçirebilirler. Uzmanlar, yaklaşan bu tehdide etkili bir şekilde karşı koymak için tüm hesaplarınızda farklı şifreler kullanma uygulamasını benimsemenizi şiddetle tavsiye ediyor.

Gelişmiş parola yönetimi için, parolalarınızı güvenli bir şekilde saklama, düzenleme ve koruma becerilerini edinmek çok önemlidir. Bu teknikleri öğrenerek şifrelerinizi daha etkin bir şekilde yönetme sürecini kolaylaştırabilirsiniz.

Uzun ve akılda kalıcı parolalar kullanın. Uzun parolalar kısa parolalara göre daha güçlüdür. Parolanız en az 12 karakter uzunluğunda olmalıdır. Parolanızda başkalarının bildiği veya kolayca bulabileceği bilgileri kullanmayın. Basit kelimelerden, yaygın ifadelerden ve kolayca tanınabilecek kalıplardan kaçınınız.

Kötü Amaçlı Yazılımlar

Bu, bir saldırganın bilgisayarınıza kötü amaçlı yazılım yüklemesini içerir. Cihazınızı bu tür saldırılara karşı korumak için antivirüs yazılımı kullanmanız ve yazılımınızı düzenli olarak güncellemeniz çok önemlidir.

Toplum Mühendisliği

Bu, bir saldırganın sizi kişisel bilgilerinizi açıklamaya ikna etmek için manipüle etmesini içerir. Bu tür bir saldırıya karşı koymak için bilinmeyen kaynaklardan gelen e-postaları dikkatlice okumak ve şüpheli görünen mesajları açmaktan kaçınmak önemlidir.

Şifre Kırma

Bu, bir saldırganın parolanızı kırarak hesabınıza erişmesini içerir. Bu tür saldırılara karşı korunmak için güçlü parolalar kullanmanız çok önemlidir. Ayrıca, iki faktörlü kimlik doğrulama uygulayarak hesaplarınızı daha da güvence altına alabilirsiniz.

Ağ Saldırıları

Bu, bir saldırganın doğrudan ağınıza veya cihazınıza saldırmasını içerir. Bu tür bir saldırıya karşı korunmak için, güvenli bir ağ kullanmak oldukça önemlidir. Ayrıca, ağınızda güvenlik duvarları uygulayarak cihazlarınızı korumak da gereklidir.

Fiziksel Hırsızlık

Bu, bir saldırganın cihazlarınızı veya diğer dijital varlıklarınızı çalmasını içerir. Ayrıca cihazlarınızı güvende tutmak için bu tür saldırılara karşı fiziksel güvenlik önlemleri almak çok önemlidir.

Dijital Varlık Güvenlik Stratejileri: Blockchain Varlıklarına Yönelik Olası Tehditler ve Geliştirilebilecek Savunma Teknikleri

Blok zinciri teknolojisi merkezi olmadığı için bazı güvenlik riskleri taşır. Blok zinciri varlıklarına yönelik olası tehditler şunlar olabilir:

%51 saldırısı

Bu, bir saldırganın blok zincirindeki işlemleri kontrol etmek için %51'den fazla bilgi işlem gücüne sahip olması gerektiği anlamına gelir. Bu gerekliliğin bir sonucu olarak, bu tür bir saldırı blok zincirindeki işlemleri manipüle etmek veya çifte harcama yapmak için kullanılabilir.

%51 saldırısı, belirli bir kripto varlığının toplam hash gücünün %51 veya daha fazlasının kontrolünü ele geçirmeyi içerir. Ve blok zinciri yapısının değiştirilmesine yol açar. Bu özel saldırı biçimi, blok zinciri teknolojilerine dayanan çok sayıda blok zinciri ağında önemli bir potansiyel tehdit olarak görülmektedir. Böyle bir saldırı, bir blok zinciri ağındaki önemli sayıda madenciyi ele geçirme kapasitesine sahiptir. Ayrıca bu durum, ağın işlemleri üzerinde kontrol sahibi olmayı sağlar. Çifte harcama ve ağın tamamen çökmesi gibi faaliyetlere imkan verebilir. %51'lik bir saldırıya karşı korunmak için, savunma teknikleri oldukça önemlidir. Bu önlemler, blok zincirindeki karma oranını yükseltmeyi kapsar. Ayrıca, blok zincirinde gerçekleşen işlemleri yakından izlemek de önemlidir. Bu platformdaki işlemlerin meşruiyetini titizlikle doğrulamak da bu önlemler arasında yer alır.

DoS (Hizmet Reddi) saldırısı

Bu, bir saldırganın blok zincirini aşırı yükleyerek işlemleri yavaşlatması veya durdurması anlamına gelir.

Bir siber saldırı türü olan Hizmet Reddi (DoS) saldırısı, bir saldırganın bilgisayar sistemlerini veya ağ kaynaklarını bozmasıyla ortaya çıkar. Bu saldırı, kullanıcı erişimini geçici ya da kalıcı olarak engelleyebilirler. Bu saldırılar, hedef sistemi aşırı taleplerle boğarak ağ kaynaklarını tüketmeyi içerir. Sonuçları ağır olabileceği gibi sistemi meşru talepleri karşılayamaz hale getirebilirler. DoS saldırılarının etkisini azaltmak için çeşitli savunma teknikleri geliştirilmiştir. Bu teknikler arasında blok zincirinin hash oranını artırmak, işlemleri yakından izlemek ve kapsamlı bir şekilde doğrulamak yer alır. Bu proaktif önlemlerin uygulanması, DoS saldırılarının olumsuz etkilerini azaltarak dijital sistemlerin bütünlüğünü koruyabilirler.

Sybil saldırısı

Bu, bir saldırganın blok zincirinde birden fazla hesap oluşturarak kontrolü ele geçirebileceği anlamına gelir.

Sybil saldırısı, bir bilgisayar ağındaki bir saldırganın ağdaki diğer kullanıcıları yanıltmak için birden fazla sahte kimlik oluşturmasıdır. Bu sahte kimliklerle ağa katılarak manipülasyon yapar. Bu tür saldırılar, ağın işleyişini bozabilirler ve ağın güvenliğini tehlikeye atabilirler. Sybil saldırılarına karşı savunma teknikleri arasında blok zincirindeki karma oranını artırmak yer alır. Ayrıca, blok zincirindeki işlemleri izlemek ve doğrulamak da bu savunma yöntemleri arasındadır.

Dijital Varlık Güvenlik Stratejileri: Akıllı sözleşmelerdeki güvenlik açıkları

Blok zinciri üzerinde çalışan akıllı sözleşmeler bazı güvenlik açıklarına sahip olabilirler. Ve bu açıklar kötü niyetli amaçlarla kullanılabilirler.

Akıllı sözleşmelerdeki yazılım hatalarından kaynaklanan bu güvenlik açıkları özellikle endişe vericidir. Bu sözleşmelerin kodundaki hatalar nedeniyle ortaya çıkarlar, bu da bu sözleşmelerin düzgün işleyişini etkileyebilirler. Akıllı sözleşmelerin doğasında bulunan güvenlik açıkları, çeşitli saldırı türlerine yol

açabilirler. Bu saldırılar, sözleşmelerin bütünlüğünü ve işlevselliğini tehlikeye atma potansiyeline sahiptir.

Bu güvenlik açıkları ışığında, savunma tekniklerinin uygulanması zorunlu hale gelmektedir. Bu yaklaşımlardan biri, akıllı sözleşmelerin doğruluk ve sağlamlıklarını sağlamak için kodlarının titizlikle hazırlanmasını içerir. Ayrıca, kodların özenle test edilmesi de bu sürecin bir parçasıdır.

Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılımlar blok zincirindeki işlemleri manipüle etmek veya çalmak için kullanılabilirler.

Bu yazılımlar, blok zincirindeki güvenliği tehlikeye atarak işlemleri değiştirme veya çalma riski taşır. Kötü amaçlı yazılımların blok zinciri üzerindeki etkisinin önemini kabul etmek, güvenliğini sağlamak için çok önemlidir. Kötü amaçlı yazılımların blok zinciri işlemlerine müdahale etmesinin potansiyel sonuçları çok büyüktür. Böyle bir saldırı yalnızca blok zincirinin sorunsuz işleyişini bozmakla kalmaz. Aynı zamanda, bu platformda gerçekleştirilen işlemlerin doğruluğunu ve bütünlüğünü de tehlikeye atma kapasitesine sahiptir.

Blok zinciri teknolojisine karşı tehditleri önlemek için uyarlanmış savunma teknikleri gereklidir. Bu önlemler, blok zincirinin karma oranını artırmayı içerebilir.Ayrıca, blok zincirinden geçen işlemleri yakından izlemek de önemlidir. Son olarak, bu yenilikçi platformdaki işlemlerin gerçekliğini titizlikle doğrulamak gerekir.

Dijital Varlık Güvenlik Stratejileri: Blockchain teknolojisi için geliştirilebilecek savunma teknikleri

Güçlü parolalar kullanın ve bunları düzenli olarak değiştirin.

Mümkün olduğunca iki faktörlü kimlik doğrulama kullanın.

Yazılımınızı güncel tutun.

Antivirüs yazılımı kullanın ve güncel tutun.

E-posta eklerini açarken veya bilinmeyen kaynaklardan gelen bağlantılara tıklarken dikkatli olun.

Halka açık Wi-Fi ağlarına bağlanırken bir VPN kullanın.

Sosyal medyada ne paylaştığınıza dikkat edin.

Verilerinizi düzenli olarak harici bir sabit diske veya bulut depolama hizmetine yedekleyin.

Şüpheli faaliyetler için hesaplarınızı izleyin.

Dijital Varlık Güvenliği Stratejileri: Sonuç

Bu makale boyunca dijital kimliğin ve dijital varlıkların tanımını kapsamlı bir şekilde inceledik. Ayrıca, tarihsel bağlamını ve gelişimini de ele aldık. Dahası, dijital kimliğimizi ve varlıklarımızı korumakla ilgili potansiyel tehditleri de inceledik. Bu zorluklara yanıt olarak, çeşitli savunma tekniklerini araştırdık. Bu tekniklerin, tehditleri etkili bir şekilde azaltmak için nasıl kullanılabileceğini değerlendirdik.

Ayrıca, blok zinciri alanına özgü potansiyel tehditleri ve savunma mekanizmalarını da özellikle belirttik. Nihai amacımız, internet kullanıcıları ve dijital varlık sahiplerinden oluşan hedef kitlemiz arasında farkındalığı arttırmaktır. Bu yüksek farkındalık sayesinde, bireylerin olası zorlukları ustalıkla aşmaları için gerekli davranış değişikliklerini teşvik ediyoruz. Bu bilgiyi aktararak, sürekli gelişen dijital ortamda güvenliği sağlamaya yönelik proaktif bir yaklaşımı desteklemeyi umuyoruz.

Teşekkür ederiz!

Co-funded by
the European Union

Blockchain Dolandırıcılığını Önleme İpuçları

Blockchain Dolandırıcılığını Önleme İpuçları rehberimize hoş geldiniz. Bu blog yazısında, blockchain dünyasındaki dolandırıcılık ve sahtekarlıklara karşı kendinizi nasıl koruyabileceğinizi ele alıyoruz. Kritik stratejiler ve içgörüler sunarak sizi yönlendireceğiz. Bu blog yazısını AB tarafından finanse edilen "V2B: Art VET Stajyerleri için Metaverse'de NFT Fırsatları Yaratmak" projesi için oluşturduk. Ve proje referans numaramız 2022-1-DE02-KA210-VET-000080828. L4Y Learning for Youth GmbH tarafından Adana Çukurova Güzel Sanatlar Lisesi ve EMC Services Ltd işbirliğiyle koordine edilen " Blockchain Dolandırıcılığını Önleme İpuçları " giriş yazısındaki eğitim çerçevesiyle ilgili olarak hazırlanmıştır.

Dolandırıcılık ve sahtekarlıklar Blockchain dünyasında nadir değildir. Kripto para birimlerinin ve merkezi olmayan sistemlerin yükselişiyle birlikte, dolandırıcılar ve sahtekarlar bireyleri sömürmek için yeni yollar belirlediler. Bu modül, bireyleri blok zinciri dünyasındaki yaygın dolandırıcılık ve sahtekarlıklar, bunların nasıl tespit edileceği ve mağdur olma tehdidini en aza indirmenin yolları hakkında eğitmeyi amaçlamaktadır. Bu modül, blok zinciri teknolojisine yatırım yapmak veya bu teknoloji ile çalışmak isteyen bireyler için tasarlanmıştır. Ayrıca, Blockchain dünyasıyla ilişkili güvenlik sorunlarını anlamak isteyen bireyler için de uygundur.

Günümüzün dijital ortamında veri ihlalleri, siber hırsızlıklar ve benzeri diğer dolandırıcılıklar açısından önemli bir risk söz konusudur. Dijital dönüşüm, dolandırıcıların yeni saldırı hatları bulmasını ve güvenlik açıklarından yararlanmasını sağlamıştır. Dolandırıcılık, iş dünyasında, özellikle de finans sektöründe her zaman zararlı bir faktör olmuştur ve işlem yaparken, sigorta başvurularını işleme koyarken, talepleri değerlendirirken veya bu tür finansal faaliyetlerde bulunurken kullanıcılarda korkuya neden olmuştur.

Blockchain Dolandırıcılığını Önleme İpuçları: Öğrenme Hedefleri

Bu modülün sonunda katılımcılar aşağıdakileri yapabileceklerdir.

- Blockchain dünyasındaki yaygın dolandırıcılık ve sahtekarlıkları tanımlamak
- Dolandırıcılar ve sahtekarlar tarafından kullanılan yöntemleri anlamak
- Yasallıklarını belirlemek için blok zinciri sistemlerini tahmin etmek

- Blockchain sistemlerinin gerçekliğini doğrulamak ve kendilerini dolandırıcılık ve sahtekarlıktan korumak için adımlar atmak.
- Blockchain güvenliği ve şık uygulamalar hakkında bir anlayış geliştirmek

Blockchain Dolandırıcılığını Önleme İpuçları: Sık Karşılaşılan Dolandırıcılıkları Anlamak

Bu bölüm, Blockchain dünyasında yaygın olan dolandırıcılık ve sahtekarlık türlerine genel bir bakış sunacaktır. Katılımcılar, dolandırıcıların ve sahtekarların bilmedikleri kişileri istismar etmek için kullandıkları yöntemleri öğreneceklerdir. Bu bölüm aynı zamanda blok zinciri teknolojisine yatırım yaparken veya bu teknolojiyle çalışırken dikkatli olmanın önemini de vurgulayacaktır.

Hadi şimdi bu unsurlara daha yakından bakalım:

1.Yaygın Dolandırıcılık ve Sahtekarlıklara Genel Bakış: Bölüm, Blockchain dünyasında yaygın olan çeşitli dolandırıcılık ve sahtekarlık türlerine geniş bir genel bakış ile açılmaktadır. Bu giriş bölümü, özellikle öğrencilerin karşılaşabilecekleri potansiyel tehditlerin kapsamını kavramalarına yardımcı olur. Belirli saldırı vektörlerini incelemeden önce risk ortamını anlamak çok önemlidir.

2.Saldırı Yöntemlerini Anlamak: Bu bölüm, dolandırıcılar ve sahtekarlar tarafından kullanılan yöntemleri detaylandırarak önemli bir adım atmaktadır. Bu bölüm, sadece tehditlerin isimlerini vermekle kalmayıp aynı zamanda bu tehditlerin nasıl işlediğine dair içgörü sağladığı için özellikle değerlidir. Ayrıca öğrenciler, kullanılan taktikleri daha iyi anlayarak bu tür saldırıları tespit etme ve azaltma becerilerini geliştirirler.

3.Tetikte Olmanın Öneminin Vurgulanması: Bu bölüm ayrıca blok zinciri teknolojisi ile uğraşırken dikkatli olmanın öneminin altını çizmektedir. Dikkatli olmaya yapılan bu vurgu, farkındalık ve proaktif güvenlik önlemlerinin blok zinciri güvenliğinin temel bileşenleri olduğunu vurgulayarak modülün gidişatını belirlemektedir.

Dolandırıcılar Blockchain Teknolojisine Nasıl Saldırırlar?

Blockchain teknolojisi güvenlik açıkları ile ilgilenmektedir. Ve dört tür saldırıya karşı savunmasızdır: kimlik avı, yönlendirme, Sybil ve %51 saldırıları.

1. Kimlik Avı

Blockchain Dolandırıcılığını Önleme İpuçları'nın önemli bir yönü, kimlik avı saldırılarını tanımak ve bunlardan kaçınmaktır. Kimlik avı saldırısı, bir saldırganın mağdurları giriş bilgileri veya finansal bilgiler gibi hassas bilgileri ifşa etmeleri için kandırmak amacıyla güvenilir bir varlık gibi davrandığı bir siber saldırı türüdür. Kimlik avı saldırıları genellikle kurbanları meşru borsalar veya cüzdanlar gibi görünen kötü amaçlı web sitelerine yönlendiren sahte bağlantılar göndererek kurbanlardan kripto para çalmak için kullanılırlar.

2. Yönlendirme Saldırısı

Yönlendirme saldırısı, bilgisayar korsanlarının internet servis sağlayıcılarına aktarılan verilere müdahale etmesidir. Bunu yaparak ağı bozabilirler ve işlemlerin tamamlanmasını engelleyebilirler. Yönlendirme saldırılarını tespit etmek ve önlemek zor olabilir. Ancak alınabilecek bazı önlemler de vardır. Örneğin, veriler gönderilmeden önce şifrelenebilirler. Ya da bağlantı noktası operatörleri şüpheli faaliyetler için ağları izleyebilirler. Mümkünse, güvenli tarafta olmak için en iyi kripto denetçilerini işe almaya çalışınız.

3. Sybil Saldırısı

Sybil saldırısında, bilgisayar korsanları birçok sahte kimlik oluşturur. Bu sahte kimliklerle ağı kalabalıklaştırır ve sistemi çökertmeye çalışır. Bu saldırı türü, Blockchain sistemlerine yönelik bir tehdittir. Bu saldırılar, birden fazla hesap, bilgisayar veya kimlik oluşturularak yapılabilmektedir. Sybil saldırıları Blockchain'e olan güveni azaltabileceği gibi finansal kayıplara da yol açabilirler. Bir Sybil

saldırısını önlemek için, güçlü güvenlik önlemlerinin alınması önemlidir. Bunlar arasında dijital imzalar veya kimlikler kullanmanın yanı sıra bilinen kimliklerin bir listesini tutmak da yer alabilir.

4. %51 Saldırısı

%51 saldırılarını anlamak, etkili Blockchain Dolandırıcılığını Önleme İpuçları için hayati önem taşır. %51 saldırısı, bir grup madencinin veya tek bir madencinin ağın madencilik gücünün %50'sinden fazlasını kontrol ettiği bir Blockchain saldırısı türüdür. Bu kontrol, defteri manipüle etmelerine olanak tanıyarak çifte harcamaya veya diğer dolandırıcılık türlerine yol açabilmektedir. %51 saldırıları çok nadir görülmekle birlikte, Blockchain güvenliği açısından ciddi bir güvenlik sorunudur.

Blockchain Dolandırıcılığının Önlenmesi için Temel Stratejiler

Bu bölümde, katılımcılar Blockchain dünyasındaki dolandırıcılık ve sahtekarlıkların nasıl tespit edileceğini öğrenme fırsatına sahip olacaklardır. Katılımcılar, takım deneyimi, teknik inceleme ve yol haritaları gibi faktörlere dayalı olarak Blockchain sistemlerini tahmin etmeyi öğreneceklerdir. Katılımcılar ayrıca Blockchain sistemlerinin yasallığını değerlendirirken dikkat etmeleri gereken tehlike işaretlerini de öğrenecekler.

Temel Blockchain Dolandırıcılığını Önleme Teknikleri

1. İki Faktörlü Kimlik Doğrulamanın Uygulanması

Blockchain alanında güvenliğin en önemli yönlerinden biri iki faktörlü kimlik doğrulamadır (2FA). 2FA'yı uygulamak, oturum açmak için şifrenize ek olarak ikinci bir faktör gerektirerek çevrimiçi hesaplarınıza ekstra bir güvenlik katmanı ekler. İkinci faktör olarak bir donanım belirteci kullanılabilir. Bu, parmak iziniz veya iris taramanız gibi biyometrik bir faktör olabilir. Alternatif olarak, bir kimlik doğrulama uygulaması tarafından oluşturulan tek seferlik bir kod da kullanılabilir.

2. Güvenilir Gönderenleri ve Alıcıları Listelemeye İzin Verin

Blockchain platformunuzu güvence altına almak için yapabileceğiniz en iyi şeylerden biri, yalnızca güvenilir göndericilere ve alıcılara izin vermektir. Bu zahmetsiz gibi görünebilir, ancak inanılmaz derecede önemlidir. Güvenilir varlıkların yalnızca Blockchain ile etkileşime girmesine izin verin. Bu, kötü niyetli faaliyet olasılığını önemli ölçüde azaltır. Tabii ki bu, Blockchain'e yeni varlıkların girmesine asla izin vermemeniz gerektiği anlamına gelmez.

3. Yazılımınızı Güncel Tutun

Bu, güvenlik güncellemelerini yüklemek ve güvenlik açıklarının keşfedilir keşfedilmez yamalanması anlamına gelir. En son güvenlik tehditlerini takip ederek, Blockchain ağınızın güvenli ve emniyetli kalmasını sağlayabilirsiniz. Ayrıca, Blockchain güvenlik ihtiyaçlarınız için saygın ve güvenilir bir sağlayıcı seçmek önemlidir. Ağlarını güvenli ve emniyetli tutma konusunda kanıtlanmış bir geçmişe sahip bir tedarikçi bulunuz.

4. VPN Kullanımı – Sanal Özel Ağ

VPN, iki cihaz arasında güvenli, şifrelenmiş bir bağlantıdır. Bu bağlantı, veri trafiğini internet gibi güvenilmeyen bir ağ üzerinden tünelleyebilir. VPN, veri trafiğini şifreleyerek bilgilerinizi kötü niyetli kişilerden korumaya yardımcı olabilir. Buna ek olarak, bir VPN gerçek IP adresinizi ve konumunuzu gizleyerek gizliliğinizi artırmayı da sağlayabilir. Pazarda birçok VPN sağlayıcısı bulunmaktadır. Ancak, güçlü şifreleme ve güvenlik özelliklerine sahip saygın bir sağlayıcı seçmek önemlidir.

5. Kimlik Avı Önleme Araçlarını Kullanma

Kimlik avı saldırıları giderek yaygınlaşmaktadır. Yani tespit edilmesi ve önlenmesi zor olabilmektedir. Bir kimlik avı önleme aracı, kimlik avı girişimlerini belirlemeye ve engellemeye yardımcı olur. Ve böylece Blockchain'inizi güvende tutabilirsiniz. Ayrıca, oltalama saldırısı belirtilerinin farkında olmak da önemlidir. Sizden bir bağlantıya tıklamanızı, kişisel bilgilerinizi vermenizi isteyen her türlü e-posta veya

mesaja şüpheyle yaklaşın. Bir e-postanın meşruluğu konusunda şüpheleriniz varsa, gerçekliğini doğrulamak için gönderenle iletişime geçin.

Uygulama Örnekleri

Katılımcılar, değerlendirme kriterlerini pratik uygulamalarla öğrenirler. Ayrıca, Ethereum ve Bitcoin gibi projeleri ve başarılı veya başarısız ICO'ları inceleyeceklerdir. Sonuçta bu vaka çalışmalarını analiz ederek, meşru Blockchain projelerinin özelliklerini ve sahte projelerin nasıl çalıştığını anlayabilirler.

Uygulama Örneği 1: Ethereum'un Başarı Hikayesi

Açıklama: Ethereum en başarılı Blockchain projelerinden biridir. Katılımcılar, Ethereum'un deneyimli ekibinin katkısını inceleyebilirler. Ayrıca, ayrıntılı teknik incelemelerin ve iyi planlanmış yol haritalarının nasıl önemli olduğunu araştırabilirler. Bu unsurların, Ethereum'un Blockchain alanındaki meşruluğuna ve önemine nasıl katkıda bulunduğunu görebilirler. Katılımcılar Ethereum'un web sitesini inceleyerek whitepaper'lara, yol haritalarına ve ekip bilgilerine erişebilirler. Ayrıca Ethereum'un geçmişini, başarılarını ve topluluk katılımını da inceleyebilirler. Yani Ethereum'un başarı öyküsü, Blockchain Dolandırıcılığını Önleme İpuçları için değerli dersler sunmaktadır.

Uygulama Örneği 2: BitConnect'in Yükselişi ve Düşüşü

Açıklama: Bitconnect, saadet zinciri olarak faaliyet gösteren hileli bir kripto para projesiydi. MEÖ öğrencileri, Bitconnect'in gerçekçi olmayan kâr iddialarını nasıl sunduğunu inceleyebilirler. Ayrıca, bu iddiaların yatırımcıları nasıl cezbettiğini analiz edebilirler. Son olarak, Bitconnect'in nasıl bir aldatmaca haline geldiğini ve çöktüğünü anlayabilirler. Bitconnect vaka çalışması, kötü şöhreti nedeniyle iyi belgelenmiştir. Bitconnect skandalını anlatan çeşitli makaleler, YouTube videoları ve haber raporları bulunmaktadır. Katılımcılar, vaka hakkında genel bir bilgi edinebilmek için bu Bitconnect Wikipedia sayfası ile başlayabilirler.

Uygulamalı Örnek 3: OneCoin Örneği

Açıklama: OneCoin, hileli bir blok zinciri projesinin bir başka kötü şöhretli örneğidir. MEÖ öğrencileri, Ruja Ignatova'nın OneCoin'in kurucusu olduğunu öğrenebilirler. Ayrıca, Ignatova'nın hayali bir blok zinciri oluşturduğunu ve sahte bir kripto para birimi çıkardığını araştırabilirler. Bu durumun, Ignatova'nın ortadan kaybolmasına ve devam eden soruşturmalara yol açtığını da inceleyebilirler. OneCoin vakası medyada geniş yer bulmuş ve yasal işlemlere konu olmuştur. Öğrenciler OneCoin dolandırıcılığının tüm kapsamını anlamak için makaleleri, belgeselleri ve haber raporlarını inceleyebilirler. Buna ek olarak, bu BBC makalesi OneCoin hikayesi hakkında ayrıntılı bilgiler sunmaktadır.

Uygulama Örneği 4: ICO Başarısızlıkları

Açıklama: MEÖ öğrencileri, Tezos ve Centra Tech gibi ICO başarısızlıklarını inceleyebilirler. Bu incelemeler, umut vaat eden blok zinciri projelerinin neden hedeflerine ulaşamadığını anlamalarına yardımcı olabilirler. Elbette bu örnekler, ekibin güvenilirliğini, teknik raporları ve yol haritalarını değerlendirmenin önemini vurgulamaktadır. Hem Tezos hem de Centra Tech, ICO faaliyetleri nedeniyle yasal zorluklarla karşılaştı. Katılımcılar, örnekleri kapsamlı şekilde anlamak için yasal işlemleri incelemelidir. Ayrıca dava gelişmelerini ve ilgili haber makalelerini de gözden geçirmelidirler. Tezos davası ve Centra Tech dolandırıcılık davası konuyla ilgili bilgi sağlamaktadır.

Yasal ve Mevzuata İlişkin Bilgiler

Blockchain alanındaki yasal ve düzenleyici ortama kısa bir genel bakış sunmak, Mesleki Eğitim ve Öğretim öğrencilerini blok zinciri teknolojisinin karmaşık dünyasında gezinme konusunda güçlendirecektir. Yani bu bölümde kripto para düzenlemeleri, devlet kurumlarının rolü ve blok zinciri projeleri için uyumluluğun önemi gibi konular ele alınacaktır. Yasal bağlamın anlaşılması, öğrencilerin düzenlemelere uyan meşru projeler ile yasaların dışında faaliyet gösteren potansiyel dolandırıcılıklar arasında ayrım yapmalarına yardımcı olacaktır.

Özetle bu bölüm, Blockchain sektöründeki temel yasal ve düzenleyici hususlara kapsamlı bir genel bakış sunmaktadır.

Kripto Para Yönetmelikleri

Genellikle 21. yüzyılın dijital altını olarak adlandırılan kripto para birimi, dünyanın dört bir yanındaki hükümetlerin ve düzenleyici kurumların büyük ilgisini çekmiştir. Yetkililer, Blockchain ve kripto para ortamının başlangıçta çok az gözetim içermesine rağmen, yatırımcıları korumak ve finansal istikrarı sürdürmek için net düzenlemeler yapma ihtiyacını giderek daha fazla kabul ettiler.

Örneğin Amerika Birleşik Devletleri, Mali Suçları Uygulama Ağı (FinCEN) ve Menkul Kıymetler ve Borsa Komisyonu (SEC) aracılığıyla kripto para birimlerini düzenlemek için adımlar atmıştır. FinCEN, kripto para borsalarında kara para aklamayı önleme (AML) ve müşterini tanı (KYC) düzenlemelerini uygulayarak şüpheli faaliyetleri ve işlemleri bildirmelerini zorunlu kılıyor. SEC, belirli kripto para birimlerini menkul kıymetler olarak kategorize etmeye ve bunları belirli düzenlemelere tabi tutmaya odaklanmaktadır.

Avrupa Birliği'ndeki Beşinci Kara Para Aklamayı Önleme Direktifi (5AMLD), kripto para borsalarının ve diğer sanal varlık hizmet sağlayıcılarının (VASP'ler) AML/CFT (kara para aklamayı önleme/terörizmin finansmanıyla mücadele) kurallarına uymasını sağlamıştır. Ayrıca yönerge, kripto para işlemlerinin şeffaflığını ve izlenebilirliğini sağlamayı amaçlıyor.

Devlet Kurumlarının Rolü

Dünya çapında devlet kurumları, Blockchain ve kripto para birimi faaliyetlerinin düzenlenmesi ve denetlenmesinde önemli bir rol oynamaktadır. Bazı önemli kurumlar şunlardır:

1.Mali Suçları Uygulama Ağı (FinCEN): Amerika Birleşik Devletleri'nde FinCEN, kripto para işletmeleri için AML ve KYC düzenlemelerini uygular. Ve ayrıca şüpheli işlemleri takip eder.

2.Menkul Kıymetler ve Borsa Komisyonu (SEC): SEC, belirli kripto para birimlerini ve ilk madeni para tekliflerini (ICO'lar) içerebilen menkul kıymetleri ve menkul kıymetlerle ilgili faaliyetleri düzenler.

3.Emtia Vadeli İşlemler Ticaret Komisyonu (CFTC): CFTC, kripto para vadeli işlemleri ve opsiyonları da dahil olmak üzere türevleri denetler.

4.İç Gelir Servisi (IRS): ABD'deki IRS, kripto para birimlerinin vergilendirilmesine ilişkin rehberlik yayınlar.

5.Avrupa Menkul Kıymetler ve Piyasalar Otoritesi (ESMA): Avrupa Birliği'nde ESMA, tokenize menkul kıymetleri de içeren menkul kıymetler piyasası için gözetim sağlar.

6.Merkez Bankaları: ABD'deki Federal Rezerv ve AB'deki Avrupa Merkez Bankası gibi merkez bankaları, kripto para birimlerinin para politikası ve finansal istikrar üzerindeki etkisini izler.

7.Finansal Denetim Otoriteleri: Birçok ülkede finansal kurumları düzenlemekten ve AML/CFT düzenlemelerine uyumu sağlamaktan sorumlu finansal denetim makamları bulunmaktadır.

Kurallara Uyumun Önemi

Yasal uyumluluk, blok zinciri alanında meşruiyetin temel taşıdır. Blockchain projeleri, güveni sağlamak için yasal ve düzenleyici gerekliliklere uymalıdır. Bu niyetle, yatırımcıların ve kullanıcıların çıkarlarını korumak için önemlidir. Uyumsuzluk yasal işlemlere, para cezalarına ve hatta bir projenin kapatılmasına neden olabilir.

Temel uyumluluk hususları arasında AML ve KYC prosedürleri, vergilendirme ve menkul kıymet düzenlemeleri yer alır. Blockchain projeleri, ICO'lar veya STO'lar yoluyla token çıkarırken menkul kıymet düzenlemelerini dikkate almalıdır. Bu projeler, tekliflerinin bu düzenlemelere uyup uymadığını kontrol etmelidir. Dahası uyumluluğu sağlamak için gerekli adımları atmalıdır.

Ayrıca, kripto para borsaları ve cüzdan sağlayıcıları belirli lisanslama ve düzenleme gerekliliklerine tabidir. Bu düzenlemeleri anlamak ve bunlara uymak hayati önem taşımaktadır. Yasal olarak faaliyet gösterebilmek ve aynı zamanda kullanıcıların fonlarını güvence altına almak için bu kurallara uymak gereklidir.

Yasal Zorluklar ve Uluslararası Varyasyonlar

Blok zinciri ve kripto para birimleri için yasal ortam sürekli olarak gelişmektedir. Ve ayrıca bir ülkeden diğerine değişmektedir. Aslında bazı ülkeler blok zincirini benimsemiştir ve net düzenlemeler oluşturmuştur. Bazı ülkeler ise şüpheci kalmakta veya yasal çerçeveler geliştirme sürecindedir.

Örneğin Malta, İsviçre ve Singapur gibi ülkelerde hükümetler Blockchain teknolojisini aktif olarak benimsemiş ve uyumluluğu korurken yeniliği teşvik etmek için düzenleyici sandbox'lar kurmuştur. Bu ülkeler blok zinciri girişimlerinin ilgisini çekmiş ve Blockchain geliştirme merkezleri haline gelmiştir.

Buna karşılık, Hindistan ve Çin gibi ülkeler temkinli davranmış, hatta sonuncusu kripto para ticaretini yasaklamıştır. Çeşitli yetki alanlarındaki yasal belirsizlikler, Blockchain projeleri ve yatırımcıları için zorluklar ve fırsatlar oluşturmaktadır.

Blockchain Dolandırıcılığını Önleme İpuçları: Sonuç

Sonuç olarak Blockchain alanındaki yasal ve düzenleyici yönler MEÖ öğrencileri için kritiktir. Kripto para düzenlemelerini ve devlet kurumlarının rollerini anlamak önemlidir. Uyumluluğun önemini kavrayarak, meşru projeler ile potansiyel dolandırıcılıkları ayırt edebilirler. Yasal sorunlar ve ülkeler arasındaki farklılıklar, Blockchain düzenlemelerinin sürekli nasıl değiştiğini göstermektedir. Bu sürekli değişen ortamda, insanların tetikte olması ve uyum sağlaması gerekir. Nihayetinde yasal gerekliliklere uyum sağlamak, projenin meşruiyetini temin eder. Aynı zamanda, blok zinciri katılımcılarının güvenliğini ve korunmasını da sağlar.

Blockchain Dolandırıcılığını Önleme İpuçları: Referanslar ve Kaynaklar

1. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-238. https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213
2. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum.
3. Hertig, A. (2021). Scams and frauds in the blockchain world: How to avoid them. CoinDesk.
4. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press. https://www.lopp.net/pdf/princeton_bitcoin_book.pdf
5. Blockchain.com, What are the most common scams? What-are-the-most-common-scams-