BLOKZİNCİR TEKNOLOJİSİ VE GERÇEK HAYAT UYGULAMALARI

INTER PROBE
INTELLIGENCE & ANALYTICS

ARALIK

Aylık Okuma Metni

HAZIRLAYAN INTERPROBE

İLGİLİ BİRİM : KRİPTOGRAFİ

Blokzincir teknolojisi, Satoshi Nakamoto'nun "Bitcoin: A Peer-to-Peer Electronic Cash System" isimli çalışması ile hayatımıza 2008 yılında girdi. Daha sonra Bitcoin, halka açık bir blok zinciri defterine ilk varlık transferini kaydederek blok zinciri teknolojisinden yararlanan ilk uygulama oldu. Çoğu insan bir süre Bitcoin ve blokzincirin aynı şey olduğunu düşündü; fakat blokzincir teknolojisi kriptoparaların ve Bitcoin'in çok ötesinde bir kavramdır. Blokzincir merkezi olmayan, değişmez ve uçtan uca dağıtılmış bir defterdir ve bu defter ağa bağlı olan çeşitli düğümlere (node) kopyalanır. Bu bakımdan blokzincir bir veri tabanı gibi düşünülebilir. Veri tabanları merkezidir ve veriler veri tabanı yöneticisi tarafından kontrol edilir ve dolayısıyla bir hata ortaya çıktığında bunun geri dönüşü olmayabilir. Diğer yandan, blokzincir merkezi olmayan ve dağıtık bir sistem olduğundan, bir düğümde ortaya çıkan bir hata diğer düğümleri ve sonuç olarak sistemi etkilemeyecektir. Blokzincirdeki veriler sadece okunabilir ve üzerine yenisi eklenebilir fakat veri tabanında veriler oluşturulabilir, okunabilir, güncellenebilir ve silinebilir. Bu tür özellikler göz önüne alındığında ikisi birbirinden oldukça farklıdır.

Blokzincir, tüm işlemlerin şeffaf olmasını sağlayarak verileri her zaman herkesin kullanımına sunar. Farklı birçok kriptografik konsept kullanılarak geliştirilmiştir. Özet fonksiyonlar, açık-gizli anahtar çiftleri ve dijital imzalar blok zincirin temelini oluşturur. Blokzincir bloklardan oluşur ve bu bloklar birbirlerine özet fonksiyonlar kullanılarak bağlanmıştır. Kullanılan sisteme bağlı olarak bloktaki veriler değişmekle beraber, genelde tek seferlik kullanılan değer, zaman damgası, henüz doğrulanmayan tüm işlemler ve bir önceki bloğun özet değeri bulunur. Tüm işlemler doğrulandıktan sonra yeni blok oluşturulur. Bu doğrulama sürecine emek ispatı (PoW) adı verilir ve bu sayede çift harcama problemi çözülür. Bir sonraki bloğu oluşturmak ve verilecek ödülü kazanmak isteyen kullanıcılara madenci denir. Madenciler, kriptografik olarak zor bir problemi çözmek için birbirleriyle yarışırlar. İçlerinden biri çözümü bulduğunda ilgili bloğu blok zincirine ekler ve ağda yayınlar. En çok bilinen konsensüs algoritmalarından biri olan PoW, ilk olarak Bitcoin'de kullanılmıştır. Fakat bütün bu Bitcoin madenciliği mekanizması, yüksek enerji tüketimi ve daha uzun bir işlem süresi gerektirir. Bu nedenle, Ethereum 2022 yılında hisse ispatını (PoS) tasarlamıştır ve bu konsensüs mekanizması emek ispatına kıyasla daha güvenlidir. Aynı zamanda daha az enerjiye ihtiyaç duyar ve yeni ölçekleme çözümlerinin daha kolay gerçeklenmesini sağlar. Buna karşın, Ethereum Classic, Monero, Dash, Zcash, Dogecoin ve diğer kriptoparalarda hala emek ispatı kullanılmaktadır.

Kriptografik özet fonksiyonları ve dijital imzalar blokzincirde önemli bir role sahiptir. Özet fonksiyonlar, blokları birbirine bağlayarak her blokta bulunan verilerin bütünlüğünü sağlar. Bloktaki en ufak bir değişiklik özet değerini tamamen değiştirdiği için blok geçersiz duruma gelir ve zincire eklenmez. Dijital imzalar, bir alıcı tarafından alınan mesajın, bilgiyi gönderdiğini iddia eden göndericiden geldiğini garanti eder. Bu özelliğe inkar edilemezlik denir. Ayrıca, mesajın alıcılara aktarımı sırasında değiştirilmediğini güvence altına alırlar. Blok zinciri tabanlı sistemler, güvenli özet alma işlemi için SHA-256 kullanırken genellikle dijital imza algoritması olarak ECDSA'yı kullanır.

Bir blok yaklaşık olarak her 10 dakikada bir üretilir. Bu nedenle, işlemlerin verimli ve güvenli bir şekilde doğrulanması gerekir. Merkle ağacı, kurcalanmaya karşı bir bileşenle verileri blokta depolamak için sıkıştıran bir veri yapısıdır. Aşağıdan yukarıya bir yaklaşımla oluşturulmuş, kurcalamaya karşı dayanıklı bir veri depolama modeli oluşturmak için her bir özet değerinin bir sonraki özet değerinin bir parçası olması kuralına dayanır. Merkle ağaçları, yalnızca bir özet değeri kalana kadar özet düğüm çiftlerinin tekrar tekrar hesaplanmasıyla oluşturulur. En son kalan özet değerine Merkle Kökü denir. Kullanıcıların bir bloğa bir işlemin dahil olup olmadığını doğrulaması için güvenli ve hızlı bir doğrulama sağlar.

Bir blokzinciri ağı çeşitli şekillerde oluşturulabilir. Herkese açık, özel, izinli veya konsorsiyum olabilirler. Herkese açık bir blok zinciri, herkesin okuma, yazma ve denetleme gibi temel faaliyetlere katılmasına ve katılmasına açıktır. Bu değişmez ve dağıtılmış ağlar, birbirine güvenmeyen ancak yine de bir ağda etkileşim kurmak ve fikir birliğine katılmak isteyen katılımcılar için idealdir. Değişmezlik, dağıtılmış defter ve kolayca giriş yapılabilmesi gibi özellikler halka açık bir blok zincirin avantajlarındandır. Ayrıca, güvenli bir herkese açık blok zincirine katılan çok sayıda kullanıcı, onu veri ihlallerinden, bilgisayar korsanlığı girişimlerinden ve diğer siber güvenlik sorunlarından korur. Bitcoin ve Ethereum, halka açık blok zincirlere örnek olarak verilebilir.

Özel bir blok zincirindeki katılımcılar, yalnızca ağa katılım için bir davet alırlarsa veya kimlikleri veya gerekli bilgileri doğrulanırsa ağa katılabilir. Ağı yalnızca bir kuruluş yönetir, kimin katılacağına karar verir, bir konsensüs protokolü uygular ve dağıtılmış kayıt defterinin devamlılığını sağlar. Deftere kimlerin yazabileceği ve hangi işlemlere katılabilecekleri gibi faaliyetler kısıtlanmıştır. Operatör yalnızca blokzincirdeki gereken girişleri geçersiz kılabilir, düzenleyebilir veya silebilir. Bu, kullanım durumuna bağlı olarak katılımcılar arasındaki güveni ve güvenilirliği artırır. Özel blokzincirler, kullanıcı kimliklerini çok fazla korumayarak şeffaflığı artırmaya odaklanır. Bunlar tedarik, finans, lojistik ve diğer iş alanları için değerli özelliklerdir. Özel bir blokzincirin diğer avantajları, uyumluluk desteğine sahip olması ve verimli konsensüs algoritmaları (BFT veya POW gibi) kullanmasıdır. Düğümler birbirlerine çok uzak konumlandırılmadığından ve sisteme katılan düğüm sayısı çok daha az olduğundan işlemler daha hızlı gerçekleşir, dolayısıyla performansı daha iyidir. IBM, Hyberledger Fabric ve Multichain, özel blok zincirlerine örnek olarak verilebilir.

İzinli blokzincirler, herkese açık ve özel blokzincirlerin bir karışımıdır. Kimliğini doğruladıktan ve belirli izinleri aldıktan sonra herkes ağa katılabilir, ancak kullanıcılar yalnızca izinlerine dayalı olarak belirli eylemleri gerçekleştirebilir. EOS ve Ripple, izinli blokzincirlere örnek olarak verilebilir.

Konsorsiyum blokzinciri herkese açık değildir ve sadece önceden seçilmiş katılımcılar kabul edilir. Bu önceden seçilmiş katılımcılar veya kuruluşlar, kimlerin işlem gönderebileceğini ve verilere erişebileceğini kontrol eder. Katılımcıların kötü niyetli davranışlar sergilediği durumda, diğer katılımcılar tarafından ağdan atılmaları mümkündür. Bu katılımcılar ağdan atılsalar bile bu durum herkese açık bir blokzincirde çok da etkili bir çözüm olmayabilir çünkü yeni kimlikler oluşturup ağa katılmak çok kolaydır. Bu nedenle konsorsiyum blok zincirleri genellikle daha küçük gruplar için kullanışlıdır. Corda ve Quorum, konsorsiyum blokzincirlere örnek olarak verilebilir.

Blockzincir teknolojisi, bir iş ağındaki işlemleri kaydetme ve varlıkları izleme sürecini basitleştirir. Bir blokzincir ağı, ilgili tüm taraflar için riski ve maliyetleri düşürerek neredeyse değeri olan her şeyi takip edebilir ve ticaretini yapabilir. Bu teknoloji, daha hızlı ve daha ucuz işlemlere, otomatikleştirilmiş sözleşmelere öncülük ederek, finansal hizmet sağlayıcılar, lojistik, otomotiv sektörleri vb. için güvenliğin artırılmasına katkı sağlar. Blokzincir teknolojisi hala yaygın olarak benimsenmese de halihazırda birçok sektör ve işletme tarafından kullanılmaktadır.

FİNANS SEKTÖRÜ

Blokzincir teknolojisi, Bitcoin'in başlangıcından beri varlıkları merkezi bir yönetime ihtiyaç duymadan taşımak için tasarlanmıştır. Blokzincir teknolojisi geliştikçe, işlemler daha hızlı ve daha ucuz hale gelmiştir. Ripple bunun en iyi bilinen bir örneğidir ve merkezi olmayan küresel bankalar ve ödeme sağlayıcıları ağı olan RippleNet için blokzincir teknolojisini kullanır. Blokzincir teknolojisini kullanan finans kurumları kullanıcılara daha hızlı gerçekleşen para transferi avantajını sağlayabilir. Bu sayede bazen saatler hatta günler süren uluslararası para transferleri çok fazla ücret ödemeden saniyeler içerisinde gerçekleşebilir.

Sözleşmeler finans sektöründe kritik öneme sahiptir ve şirketler bunlara önemli ölçüde zaman harcarlar. Akıllı sözleşmelerle bu süreci kısaltmak ve verimli hale getirmek mümkün hale gelmiştir. Akıllı sözleşme, sözleşmeye dayalı anlaşmaları uygulayabilen bir blokzinciri üzerinde çalışan bir programdır. Genellikle bir dizi kuralı uygulayan dijital anlaşmalar olarak düşünülebilir. Bu kurallar, ağdaki düğümler tarafından çoğaltılan ve yürütülen bilgisayar kodu tarafından önceden tanımlanmıştır. Örneğin bir sigorta şirketi, talep sürecini hızlandırmak için akıllı sözleşmeleri kullanabilir. Bir müşteri bir talep gönderdiğinde, kodlar tarafından otomatik olarak incelenir ve talep geçerliyse şirket müşteriye ödeme yapar.

TEDARİK ZİNCİRİ

Akıllı sensörler ve RFID etiketleri gibi IoT cihazları, belirli ürünler tedarik zincirinin çeşitli aşamalarından geçerken durumlarının ne olduğunu (sıcaklık, titreşim, nem vb.) verimli bir şekilde kaydedebilir. Böylece şirketler sorunları kolayca anlayabilir ve hızlı bir şekilde tespit edebilir. Ayrıca bu durum olası maliyet tasarruflarına da işaret eder. Yediğimiz çoğu gıda üretim, işleme, paketleme, depolama ve dağıtım ağını içeren karmaşık bir küresel tedarik zincirinin sonucudur. Ayrıca insanlar piyasada gördükleri veya sofralarına gelen gıdaların ne zaman üretildiğini, hangi koşullarda taşındığını ve taşınırken bozulup bozulmadığını blokzincir teknolojisi sayesinde öğrenebilirler. Çapraz kontaminasyon ve hastalık bulaşması gibi birçok gıda güvenliği sorunlarını izlemek ve belirlemek zordur. Blokzincirin doğruluğu ve bütünlüğü, bu sorunları ele almak için özellikle uygun olmasını sağlar. 2017 yılından bu yana sadece gıda sektörü değil, diğer sektörlerden şirketler de blokzinciri sistemlerine entegre ederek bu tür sorunlara çözüm üretmeye çalışmaktadır.

SAĞLIK

Sağlık sektöründe blokzincir altyapısının kullanılmasıyla birlikte bazı süreçlerin hızlandığı ve risklerin en aza indirildiği gözlemlenmiştir. Örneğin, hastaneler hasta kaydı sırasında hastaların adres bilgilerini isterler ve bu bilgileri kayıt altında tutarlar. Hasta bir yerden başka bir yere taşındığında tüm hastanelerin kayıtlarındaki eski adresini güncelleyemez. Sağlık alanında aynı bilgileri tekrar tekrar sağlamak zorunda kalmak ve güncellemek hastaların karşılaştığı en yorucu ve takibinin de güç olduğu şeylerden biridir. Bu nedenle, hastaların bilgilerini tek bir yerden güncellemesi ve bu bilgilerin sistem genelinde otomatik olarak yenilenmesi herkesin işini kolaylaştıracaktır. Ayrıca, hastaların kullandığı ilaçların orijinal olması ve ilacın bileşenlerinin olması gerektiği gibi olması önemlidir. Aşılar gibi bazı ilaçlar özel taşıma koşullarına ihtiyaç duyar. Bu nedenle, taşıma esnasında sağlanan koşullarda çok fazla dalgalanma olmaması gerekir. Blokzincir teknolojisi, tasarruf ederek ve kritik kaynaklara ek yatırımı teşvik ederek küresel sağlık sektörünün gelişimini desteklemeye yardımcı olabilir.

Blokzincir teknolojisi, üzerinde çalışmak ve geliştirmek için geleceği parlak bir alandır. Durum böyle olsa bile her iş alanı için uygun olmayabilir. Bu nedenle blokzinciri bir işletmeye entegre etmeden önce bazı soruları yanıtlamak ve sistem gereksinimlerini göz önünde bulundurmak işletme için doğru kararın verilmesinde yardımcı olacaktır.

KAYNAKLAR

https://builtin.com/blockchain/blockchain-in-supply-chain
https://www.ibm.com/topics/what-is-blockchain
https://medium.com/swlh/a-simple-guide-to-understanding-blockchain-8dd09356b153
https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-in-finance/
https://www.mongodb.com/databases/blockchain-database
https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/