Blok Zinciri ve Siber Güvenlik

Derleyen: Ahmet Kaşif

Kripto Paralar

İlk kripto para olan Bitcoin'in mucidi Satoshi Nakamoto, bu yeni kavramı ilk duyurduğu 2008'deki tanıtımda, Bitcoin'den "uçtan uca elektronik para sistemi" (P2P) olarak bahsediyor.

90'lardaki merkezileştirilmiş dijital paralardan farkı ve ortaya atıldığı günden bu yana yaşayabiliyor olması, dağıtık bir sistem kullanan blok zinciri temelli olmasına bağlanırken, teoride kripto paralar hiçbir finans otoritesi veya devlet tarafından denetlenmemekte ve gerçek paralar gibi altın rezervlerine bir bağımlılığa sahip olmamaktadır.

Bitcoin'in başarısı üzerine dijital para ağı genişleyip çeşitlendi. 2017 yılında bu tür dijital paraları kabul eden Coin Market Cap borsasının, 1325 farklı kripto parayla işlem yapmaya devam ettiği belirtiliyor.

Kripto Paralar

Kripto paralar şu ifadeyle tanımlanıyor :

“Bir veri tabanında, belirli şartlar sağlanmadan değiştirilemeyen sınırlı sayıda girdi.”

Blok Zinciri

Blok zinciri, kripto paraların var olmasını sağlayan ve tüm kripto paraların altında yatan teknolojidir. Zamana göre sıralanmış ve sürekli büyüyen bir veri yapısı olarak nitelendirilen blok zincirinde bloklar, yapılan işlemleri ve bir önceki blokun adresini tutarlar. Dolayısıyla blok zinciri, işlemler listesini barındıran dev bir kayıt defteridir (ledger).

Blok zincirinde kayıtlar birbirlerine çeşitli matematiksel işlemler ile (kriptografi) bağlanırlar.

Bitcoin'in ortaya çıkmasıyla tanıtılmış ve kullanılmaya başlanmış olup, dağıtık bir sistemdir, sistem içerisindeki herkes verilere erişebilir. Veriler şifreli bir şekilde tutularak, üzerinde değişiklik yapılması engellenir ve tüm kullanıcılar gizli kalır.

Blok Zinciri - Temel Kavramlar

Madenci Düğümü : İşlemlerin gerçekleştiği bilgisayarlardır. Önceleri bilgisayarların ana işlem birimleri kullanılırken, son dönemde blok zinciri işlemlerinde daha verimli çalıştığı gözlenen grafik kartı işlemcileri veya özel üretim işlemciler kullanılmaya başlanmıştır.

Madencilik Gücü : Bir makinenin işlem gücünü temsil eden madencilik gücü, saniyede işlenen özet (hash) sayısı ile ifade edilir. (H/s) Makinelerin madencilik gücünün artırımı için, birkaç işlemcinin ortak kullanımı değerlendirilebilmektedir.

Blok Zinciri - Temel Kavramlar

1. Blok zincirinin tüm düğümlerde aynı olabilmesi için değişiklik yapacak olan cihazı belirleyen kurallar bütünüdür.
2. Temel yaklaşımlar arasında, PoW ve PoS yaklaşımları bulunmaktadır.

Pow (Proof of Work) - Pos (Proof of Stake)

Proof Of Work :

Her düğümün, çalışmadan önce çalışmayı hak ettiğini gösteren, çözmesi gereken problemdir. Dışarıdan çözülmesi zor, fakat işleyen cihaz tarafından rahatça çözülebilecek bir değerdir.

Proof of Stake :

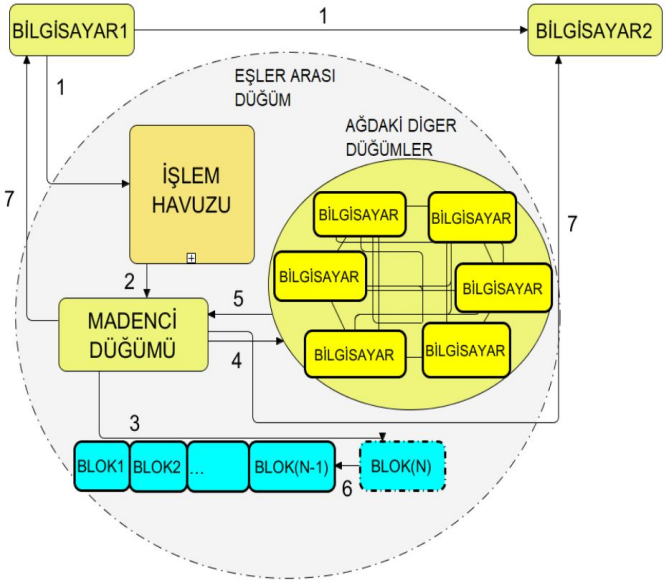
Çözülmesi gereken bir problem yerine, sistemin sahip olduğu kripto para zenginliğine göre cihazın seçilmesine dayanır.

Blok Zinciri - Genel Özellikler

1. Merkezi değildir.
2. İşlemler, P2P ağda tüm düğümlere yayınlanır.
3. İşlemler birden fazla düğüm tarafından onaylanır.
4. Sistemdeki tüm hesaplar halka açıktır fakat aynı zamanda anonimdir, hesap kimlik numarası aynı zamanda açık anahtardır(public key).

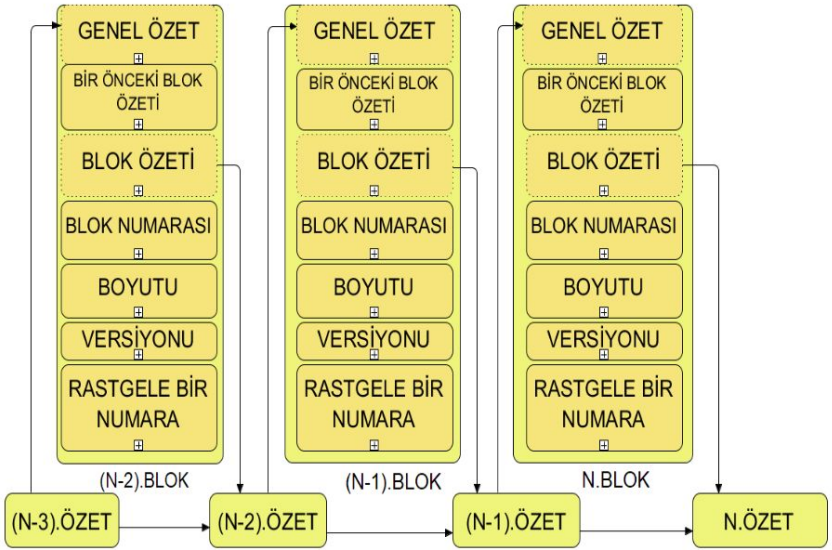
Blok Zinciri - Örnek İşleyiş

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



Blok Zinciri Yapısı

Bloklar, hash (özet) değeri ile önceki bloklara bağlanmaktadır. Bu süreçte önceki bloklardaki özet değerinden genel özet değeri oluşturulmakta ve aynı zamanda bir önceki blokun özeti de saklanmaktadır.



Blok Zinciri - Güvenlik

Saldırganların sistemi ele geçirebilmesi için, ağdaki düğümlerin çoğunu ele geçirmesi gerekmektedir. Düğümlerin dağıtık olması, bu olasılığı en aza indirmektedir.

Blok zinciri yapısında hash fonksiyonları aktif olarak kullanılmaktadır. Her blok kendinden önceki blokun sağlamasını (hash) tutar. Hash fonksiyonu olarak farklı algoritmalar kullanılmakla birlikte, BTC SHA256 algoritmasını kullanmaktadır.

Sistemdeki bir işlemi değiştirmek, zincirdeki tüm blokları değiştirmek demektir ve bu muazzam bir işlem gücüne ihtiyaç duyar. Teorik olarak mümkün bir saldırı olsa da, henüz pratik olarak bu işlem gücünün toplanılarak saldırı düzenlenmesi olası görülmemektedir.

Blok Zinciri - Güvenlik Servisleri

Blok zinciri, veri bütünlüğünü ve kullanılabilirliği arttırmayı, hata toleransını en azda tutmayı hedefler. Gizlilik servisini ise doğrudan hedeflemez, verileri açık tutar. Verilerin açık tutulması, kime ait olduklarının bilinmemesinden dolayı gizlilik tabanlı işlemlere de fırsat sunmaktadır.

Blok Zinciri - Başlıca Sorunlar

1. İşlemlerin kayıt altında tutulduğu blokların büyümesi ve bu nedenle performansın düşmesi
2. Büyük miktarlarda madenci düğümü kuran şirketlerin sistemde baskın güce erişme riski
3. Yüksek enerji (elektrik) isterleri

Blok Zinciri - Sorunlar ve Çözüm Yaklaşımları

Daha hızlı ve ölçeklenebilir “Lightning Network” çözümü ile performans gerektiren özelliklerin devre dışı bırakılarak sürecin yönetilmesi ve IOT seviyesine de uyarlanabilmesi hedeflenmektedir.

PoW yaklaşımı yerine PoS yaklaşımı çalışılmakta ve matematiksel problem çözümü için harcanan işlemci gücü yerine rastlantısal seçim kullanarak enerji tasarrufu düşünülmektedir.

Kaynaklar

1. Kaynak Makale (Son Erişim: 21.03.2018)
2. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (Son Erişim: 21.03.2018)
3. https://blockgeeks.com/guides/what-is-cryptocurrency/ (Son Erişim: 21.03.2018)

Teşekkürler