Blokzincir: Beklentiler ve Gerçekler

Ali Aydın Selçuk
TOBB-ETÜ

Blokzincir: Büyük Beklentiler

- Son yılların en çok konuşulan teknolojisi.

- "[Blokzincir] önümüzdeki on yıl için düşünebildiğimiz en büyük fırsat kümesidir."
  – Bob Greifeld, NASDAQ (eski) CEO'su
- "Bundan 20 yıl sonra geriye dönüp bakacağız ve Bitcoin'in yenilikler için en az İnternet'in kendisi kadar etkili bir platform olduğunu göreceğiz."
  – Marc Andreessen, WWW öncüsü, yatırımcı

Blokzincir: Büyük Beklentiler

- “Bitcoin dünya tarihinde İnternet’ten sonraki en önemli icattır.”
  – Roger Ver, Bitcoin yatırımcısı
- “Sanal paraların uzun vadede geleceği olabilir, özellikle de yenilikler daha hızlı, daha güvenli, daha verimli bir ödeme yöntemi sunarsa.”
  – Ben Bernanke, Fed (eski) başkanı
- “Blokzincir sadece bir devrim olarak tanımlanamaz. O tsunami benzeri bir fenomendir.”
  – William Mougayar, yazar

Peki Blokzincir Nedir?

- Özünde, P2P ağ üzerinde paylaşılan dağıtık bir defterdir.
- Sistemdeki her kullanıcı defterin bir kopyasını tutar, ve yapılan işlemler düzenli olarak deftere işlenir.
- Kullanıcı kopyaları arasında uyumsuzluk olması durumunda bunu çözecek bir otorite bulunmaz.
- Bunun yerine tutarlılık, bir uzlaşma algoritması tarafından sağlanır.
- Yeni kayıtlar deftere uzlaşmayla beraber "blok" (~sayfa) halinde işlenir.

Uzlaşma Algoritmaları

- Blokzincir teknolojisinin en ilginç parçası.
- Değişik alternetifler: PoW, PoS, BFT, …

- Emek İspatı (PoW)
  - Blok ekleme işlemi, sistem tarafından kasıtlı olarak yavaşlatılır.
  - Yeni blok eklemek için bir bulmacanın çözülmesi gereklidir.
  - Eşitlik durumunda uzlaşma, fazladan emek harcayarak sağlanır.
  - Yan etki: korkunç kaynak israfı

Uzlaşma Algoritmaları

- Hisse İspatı (PoS)
  - Madenciler bu iş için sistemdeki varlıklarını yatırır.
  - PoW ile bir arada kullanılabilir.
  - PoW ile israf olacak kaynaklar korunmuş olur.
- Bizans Hata Toleransı (BFT)
  - Küçük, seçkin bir grup kullanıcı kendi aralarında haberleşir ve yeni blokları onaylar.
  - Çok verimlidir.
  - Soru: Uzlaşma grubunda hangi kullanıcılar yer alacak?

Blokzincirin Vadettikleri

- Dağıtık açık defter
- Dijital veri
- Gerçek zamanda güncelleme
- Kronolojik sıralı ve zaman damgalı
- Kriptografik olarak mühürlü
- Tersine çevrilemez, denetlenebilir
- Güvenilir otorite olmadan çalışır

- Güvenilir otorite olmadan çalışan güvenilir bir sistem! (bir kripto-anarşistin rüyası)

Etkilenmesi Beklenen Sektörler

- Finans işlemleri
- Tedaik zinciri yönetimi
- Sağlık yönetimi
- Belge doğrulama (ehliyet, diploma)
- Dijital oylama
- …

Furya (Hype)

- Bitcoin'in sansasyonel başarısından sonra blokzincir, "bir sonraki büyük icat" olarak görüldü.
- Bir furya yaşandı:
  - Long Island Ice Tea şirketi ismini Long Blockchain olarak değiştirdi ve hisseleri $2.44'den $6.91'e fırladı, Aralık 2017'de.
  - Kodak şirketi KODAKCoin isminde bir kriptopara çalışması duyurdu ve hisseleri $3.10'den $9.20'e fırladı, Ocak 2018'de (daha sonra ~$2.40, Ekim 2018'de).

Furya

- Büyük miktarda yatırım blokzincir projelerine aktı, furya daha da büyüdü.
- “Blokzincir” kelimesi, anlamlı anlamsız herşey ile tamlama yapar oldu.
- 1990’ların sonundaki dot-com furyasını hatırlatan bir dönem yaşandı.
- Herkes blokzincir için “çarpıcı uygulama” bulma peşine düştü.

Tereddütler

- Bitcoin yaklaşık on, Ethereum da beş yıldır var. Yıllardır da blokzincirin büyük potansiyelinden söz ediliyor.
- Hala sözü edilen çarpıcı uygulamalar görülemedi.
- Blokzincir gitgide problem arayışında olan bir çözüm izlenimi veriyor.
- Sanıldığının aksine, insanlar otoriteden nefret edip tamamen merkezsizleştirilmiş sistemler istemiyor.

Eleştirel Bir Bakış

- İstenen çözümle ilgili varsayımlarımızı sorgulamalıyız.
- Gerçek hayattaki çoğu problem merkezsiz bir çözüm aramaz, ve istemci-sunucu mimarisi ile daha kolay çözülebilir.
- Aslında, güvenilir bir otoritenin varlığı, anlaşmazlık durumlarında çoğu insan için istenen bir özelliktir.
- Doğrusu, otoriteye tamamen karşı olan anarşist görüş, toplumda küçük bir azınlıktır.

Eleştirel Bir Bakış

- Blokzincir sistemlerindeki güzel bir çok özellik aslında içinde bulunan diğer işlevlerden gelir:
  - dijitalleştirilmiş veri
  - düzenli veri girişi
  - PKI
  - çevrimiçi hizmet

- Benzer varsayımlarla, bir istemci-sunucu çözümü, daha kolaya ve ucuza kurulup işletilebilir.

Örnek: Tedarik Zinciri

- Walmart geçen aylarda sebze-meyve ürünlerini blokzincir üzerinden takip edeceği bir sistemi duyurdu.
- Gıda güvenliği için ürünler tarladan reyona kadar takip edilecek.
- Aslında, Walmart 2006'da da benzer bir program başlatmıştı, ancak kullanıcıların veri girişindeki sorunlardan dolayı program 2009'da terk edilmişti.
- Peki şimdi neden sunucu yerine blokzincir?

Örnek: Sürücü Ehliyeti

- Florida eyaleti, sürücü ehliyetlerinin blokzincir üzerinde tutulacağı bir proje açıkladı.
- Böylece polis memurları ehliyet kayıtlarına çevrimiçi olarak 7/24 her yerden erişebilecekler.
- Fakat blokzincirin bu işle ne alakası var?

Örnek: Akademik Belgeler

- Üniversiteler öğrenci belgelerini (transkript, diploma, vs.) blokzincir üzerinde tutar; böylece çevrimiçi olarak her yerden erişilebilir.
- Üniversite veya bir kamu kurumu tarafından çalıştırılacak bir sunucu daha kolay olurdu, ancak blokzincirin de avantajları var.
- Blokzincirin avantajları:
  - Çevrimiçi, bütünleşik bir veritabanı.
  - Bir üniversite kapansa bile belgelerine erişilebilir. (?)
  - Üniversite tarafından suistimale karşı koruma. (?)

Örnek: Roaming Ücretlendirme

- GSM roaming ücretlendirmesinde, ziyaret edilen operatör (VPMN) home operatöre (HPMN) kullanım kayıtlarını gönderir.
- Kayıtlar arasında farklılık olabilir ve bunun çözülmesi gerekir. Sonra hesap kapatılır.
- Blokzincir: anında çözüm!
- Aslında değil: Zaten girilecek veri konusunda uzlaşamıyorlar!

Örnek: Seçim Güvenliği

- Seçim sonuçları bazen tartışmalı olabiliyor (örneğin, ABD 2000).
- Blokzincir, kayıtların saklanması için kurcalamaya karşı dayanıklı bir yöntem sunar.
- Tam çözüm değil: Seçimlerde sahtecilik olursa, kayıtlar girilmeden *önce* olur.

Örnek: Akıllı Sözleşmeler

- Akıllı sözleşme: “Program kanundur.”
- Sözleşme, bir programlama dilinde kodlanır ve blokzincirde saklanır.
- Belli bir şart gerçekleştiğinde (bu bir “aygıt” tarafından da tetiklenebilir) blokzincirde ödeme yapılır.
- “Aygıt” gerçek dünyadaki olayların (konum, sıcaklık, veya çevrimiçi bir olay gibi) bilgisini blokzincire, güvenilir bir şekilde aktarır.

Örnek: Akıllı Sözleşmeler

- Akıllı sözleşmeler, şu anda yasal anlamda sözleşme değiller.
- Yasal düzenlemeler kolay veya yakın gözükmüyor.
- Nitelikli imza için gereken düzenlemeleri hatırlayın.
- Görünür gelecek için: “Program kanundur.”

Eleştirel Bir Bakış (tekrar)

- İstenen çözümle ilgili varsayımlarımızı sorgulamalıyız.
- Gerçek hayattaki çoğu problem merkezsiz bir çözüm aramaz, ve istemci-sunucu mimarisi ile daha kolay çözülebilir.
- Aslında, güvenilir bir otoritenin varlığı, anlaşmazlık durumlarında çoğu insan için istenen bir özelliktir.
- Doğrusu, otoriteye tamamen karşı olan anarşist görüş, toplumda küçük bir azınlıktır.

Eleştirel Bir Bakış (tekrar)

- Blokzincir sistemlerindeki güzel bir çok özellik aslında içinde bulunan diğer işlevlerden gelir:
  - dijitalleştirilmiş veri
  - düzenli veri girişi
  - PKI
  - çevrimiçi hizmet
- Benzer varsayımlarla, bir istemci-sunucu çözümü, daha kolaya ve ucuza kurulup işletilebilir.

Şüpheci Bakış

- Ortada bir furya olduğu anlaşıldıkça şüpheci bakış daha çok seslendirilir oldu:
  - “Blokzincirin tek makul uygulaması elektronik paradır.” (J. Song)
  - “Blokzincir faydasız bir teknolojidir.” (N. Roubini)

- Katılmıyorum. Orta nokta mümkün.

Dengeli Bakış

- Blokzincir,
  - faydasız bir teknoloji değildir,
  - ama İnternet'ten sonraki en büyük icat da değildir.
- Blokzincir, güzel özellikleri olan önemli bir icattır.
- Fakat gerçek hayatta, tamamen merkezsiz bir sistem için talep fazla değil.

Makul Uygulama Alanları

- Blokzincir bir çok durumda farklı kurumların veritabanlarını, çevrimiçi hizmet için entegre etmenin bir yolu olarak görülüyor.
- Güvenilir bir otoritenin olmadığı durumlardaki uygulamalar daha anlamlı oluyor.
  - sağlık veritabanı, ABD ve Türkiye
  - diploma veritabanı, ABD ve Türkiye
- Güvenilir otoritenin olduğu durumda benzer bir hizmet çok daha kolay ve ucuza sağlanabilir.
- Uluslararası uygulamalar genellikle ulusal uygulamalardan daha anlamlı oluyor.

Makul Uygulama Alanları

- Uluslararası para transferi
  - Ripple & Stellar gibi blokzincir sistemleri SWIFT, MoneyGram, Western Union'a alternatif durumunda.
- Uluslararası çevre koruma
  - Sensörler, ortak bir veritabanına kısıtlama olmadan veri girişi yapacaklar.
- Eczacılık sektörü: ilaç tedarik zinciri
  - İlaç Tedarik Zinciri Güvenliği Yasası, ABD, 2013
  - Şirketlerin ve tedarikçilerin, ilaçların nerelerde üretildiğini, dağıtıldığını, satıldığını takip etmesi gerekecek, 2020.
  - Merkezsiz bir veritabanı faydalı olabilir.

Kripto Para Üzerine Düşünceler

- Bu tamamen farklı bir olay. Burada blokzincir sadece alttaki teknoloji.
- Bernanke'nin dediğini hatırlayın:
  "Sanal paraların uzun vadede geleceği olabilir, özellikle de yenilikler daha hızlı, daha güvenli, daha verimli bir ödeme yöntemi sunarsa."
- Paranın tarihindeki bir sonraki büyük buluş olabilir, belki.

Kripto Para Üzerine Düşünceler

Paranın kısa tarihi:

- takas
- emtia para (tuz, çiftlik hayvanları)
- kıymetli madenler (altın, gümüş)
- kağıt para
- elektronik ödeme
- kripto para (?)

Olabilir. Kesin bir şey söylemek zor. Kağıt para altının yerini alırken de insanlar şüpheci yaklaşmıştı. Gelecek nesiller karar verecek.

Blokzincirin Yaygınlaşması Önündeki Problemler

Onca yıllık çalışma, onca yatırım, ve onca ürün önerisinden sonra, neden hala blokzincirin yaygın kullanımını görmüyoruz?

- Acil ihtiyaç duyulmaması
  - Blokzincirin bazı artıları olsa da sunucu çözümleri, çoğu durumda %99 istenen faydayı sağlıyor.
- Kavrama ve güven noktasında sorular
  - Blokzincirin güvenlik özelliklerini kavramak bilgisayarcılar için bile zor.
- Siber güvenlikle ilgili tereddütler
  - 2018'deki hırsızlık ~1 milyar dolar.
- Yasal düzenleme bulunmaması

Furyanın Ötesinde

- Blokzincir sadece bir furya değil, güzel özellikleri olan önemli bir icat:
  - dağıtık açık defter,
  - değiştilemez & denetlenebilir.
- Fakat önerilen uygulamalar iyi sorgulanmalı:
  - Merkezsiz bir çözüm gerekli mi?
  - Hangi risklere karşı koruma sağlar?
  - Aynı varsayımlarla (dijital veri, PKI), sunucu-istemci çözümü ne kadar iş görür?
- Bu sorulara tatminkar cevap verebilen uygulamaların başarı şansı olur.

Sonuçlar

- Blokzincir özgün bir teknoloji.
- Fakat son yıllarda abartılı bir furyanın konusu olmuş durumda.
- İşler normale dönecek ve blokzincirin gerçek uygulamalarını göreceğiz.
- 1990'lardaki dot-com furyasını hatırlayın:
  - Balon patladı ve kurulan şirketlerin %99'u yok oldu.
  - Fakat geriye kalan sağlamları, Amazon ve Google gibi, gerçekten de dünyayı değiştirdiler.
- Tarih tekerrür edecek mi?