

CMPE 444 DERSİ İÇİN NOTLAR:

cemil ş. türün

1-BTC (bitcoin) özelinde incelediğimiz konular:

- a) akarca/**currency** olup olamayacağı,
- b) emtia/commodity olup olmadığı,
- c) menkul değer/security olup olmadığı.

BTC'nin currency olması konusunda sorun, işlem süresinin uzunluğu, yani 10 dakikada bir defa onay alınıyor olması. Bu süre çok uzun, karşılaştırmak için: Visa network'u saniyede 5000-8000 işlem yapabiliyor.

Ethereum daha hızlı işleme izin veriyor. Ancak onda da hızlar henüz yeterli değil. On-chain diye bir kavram var, rakibi kavram: off-chain. Off-chain, gerçek ethereum main network'une işlenmeyen, virtual olarak yapılan işlemlere deniyor.

Şu anda BTC daha çok bir dijital emtia gibi davranıyor. Dolar gibi fiat paralara alternatif olarak yatırım aracı gibi işlevi var. Commodity: altın gümüş, demir, fındık gibi meta'lara deniliyor. Meta kelimesinin çoğulu emtia. Metalar = emtia.

Üçüncü olarak, BTC'nin ya da Ether'in menkul kıymet olarak nasıl işlem görebileceği meselesi var. Şu anda token ekosistemindeki alt-coin'lerin çoğu aslında birer şirket/proje. Bu projelerin yatırımını BTC ve Ether paraları kullanarak yapıyoruz. Yani, her projenin coin'i ya da token'ı o projenin **hisse senedi** işlevini görüyor.

Şu anda, geleneksel dünyada hisse senedi işlemleri sadece özel izin verilen Borsa adlı merkezi birimlerde yapılıyor. Türkiye'de borsanın adı: BİST (Borsa İstanbul). BİST bünyesinde Borsa dışında iki kurum daha var, daha doğrusu Borsamız aslında 3 kurumun bileşiminden oluşuyor: Borsa (alım-satım yapılan pazaryeri), MKK (merkezi kayıt kuruluşu) ki burada tüm hisse senetlerinin kaydı database'lerde tutuluyor ve son olarak Takasbank, bu kurum da alım satımı yapılan hisse senetlerinin el değiştirmesinde paraların el değiştirmesini yapıyor.

Borsada hisse senetleri dışında enerji değiş-tokuş işlemleri, altın değiş-tokuşu ve hatta tapu değiş tokuşu da yapılıyor. Tüm işlemler MKK'da kayıtlı dijital veriler üzerinden yapılıyor. Mesela Koç Holding'in hissesini almak isteyen birisi, önce İş Yatırım, Ak Yatırım, Gedik Yatırım filan gibi yerlerde önce hesap açtırmak zorunda. Bunlara aracı kurum deniliyor. Borsada işlem yapma yetkisi sadece bu aracı kurumlara verilmiş.

Bu merkezi yapıya alternatif olabilecek şekilde alt-coin'ler tamamen dağıtık (decentralized) bir şekilde işliyor. Aracı kurum diye bir şey yok. Herkes kendisi alt-coin ya da alt-token satın alıp o projeye yatırımcı olabilir. Bu "hisse"ler şu anda iki şekilde el değiştirebiliyor: 1- Crypto borsalarda 2- Doğrudan projenin yazılımını kurarak kendi bilgisayarınızda. Bu ikinci seçenek sadece ICO denilen Coin Halka Arzı zamanlarından mümkün olabiliyor. ICO zamanını geçirdiğinizde ise tek seçeneğiniz o token'ları "mine etmek" (madencilikini yapmak) ya da borsalardan BTC veya Ether karşılığı olarak değiş-tokuş etmek.

Crypto borsalardan Ether veya BTC satın almak isteyen birisi, TL ya da dolar (USD) ödeyebiliyor. Bu durumda crypto borsasında hesap açmanız gerekiyor. Bu açıdan şu anda bu kripto-borsalar merkezi sistemdeki borsaları andırıyor. Ancak bunlar şu anda regülasyona yani denetlemeye tabi değiller. Kanunsuz da değiller ama paranızı kaybederseniz hukuki sorumluluk taşıyan birisini bulamıyorsunuz karşınızda.

2- ICO: Initial Coin Offering demek. Bu kelimenin merkezi sistemdeki eşleniği IPO.

IPO, Initial Public Offering, Türkçesi ile halka arz demek. Şirketlerin Borsa üzerinden halka açılması ve hisselerinin kamuya satılması.

Bu ikisi arasındaki önemli farklar şunlar:

— Halka arz, bir şirket karlı hale geldiği, büyüdüğü zaman, daha da büyümek için sermaye arttıracığında oluyor. Masraflı bir iş. Bu halka arz etme işlemini sadece yetkili bankalar ve aracı kurumlar yapabiliyor. Elitist bir tarafı var.

— ICO ise daha proje işin başındayken yapılabiliyor. Daha doğrusu çoğunlukla ICO yapanlar bu şekilde henüz işin başında olan projeler. Bunlar şirket bile olmayabiliyorlar. Tabii ki bunlara para yatırmak isteyenler risk alıyorlar ve regülasyon (kanuni düzenleme) olmayan bir alanda oynuyorlar. Bir tür kumara benziyor. Gerçekten anlamlı projeler de var ICO yapmış olan.

— Şu anda dünyada ICO salgını durulmuş durumda. Daha çok önden “private sale” denilen az sayıda büyük yatırımcıya satış yapıldığı görülüyor. Kanuni olarak sorunlar olması da dünyada ICO’ları yavaşlattı. Malta ve Cebelitarık gibi bir kaç ülkede hala ICO yapılabiliyor.

— Ne var ki ICO’lar eğer risklerinden bir miktar arındırılabilirse, ki tamamen risksiz yatırım diye bir şey olamaz, o zaman kurumların halka arzı hem tabana yayılmış olur hem de kolaylaşır.

— Bugün ICO’lara en yakın kanuni para toplama yöntemine “crowd funding” ya da “kitlesel fonlama” deniyor. Kickstarter en önemli örneği.

— Şu anda IPO’lar masraflı ve pazar koşulları da uygun olmadığından çok fazla şirket dünyada halka arz edilmiyor. Sadece çok iddialı veya gerçekten yüksek ciro lu firmalar bu işe kalkışıyor. Mesela SNAP geçen sene iddialı bir IPO yaptı. IPO’lar için fiat currency (devlet paraları) kullanılıyor; ICO’lar için ise kripto-asetler.

3- Diğer Kavramlar:

KYC: Know Your Customer. Müşterinin kim olduğu biliniyor, anonim işlem yok demek.

AML : Anti Money Laundering , yani para aklamaya karşı kurallar seti demek.

Consensus: Mutabakat.

DLT: Eğer blockchain private yani özel ise (hususî de denilebilir) bu durumda DLT veya “private blockchain” demeyi tercih ediyoruz.

Blockchain: Bu kavramı tamamen “decentralized” ve “public” yani kamusal blokzinciri için kullanacağız.

Peer-to-peer (bazen peer-2-peer veya p2p olarak da yazılır) = eşten eşe olarak çeviriyoruz.

Point-to-point ise uçtan uca olarak çeviriyoruz.

Public: Kamusal demek. **Kamu** da Türkçe **halk** demek.

Trust= Güven, Security = Emniyet demek.

Vadeli çekler (**VÇ**), dağıtık ve decentralized (merkezi olmayan) bir blokzinciri şeklinde çalışıyor.

Vadeli çeklere benzer başka enstrümanlar da şunlar: Senetler ve faturalı açık hesaplar.

Bu enstrüman Türkiye’ye özgü, dünyada başka ülkelerde bir benzeri yok. **VÇ**, vatandaşın para yaratabilmesini mümkün kılıyor. Elden ele geçen VÇ’ler, üzerlerindeki değerin çok üstünde, vade süresi içinde değiştirdikleri el sayısı kadar çarpanlı bir ekonomi oluşmasına sebep oluyorlar. Bu mekanizma bankaların dışında çalışıyor, bankaların kurduğu ya da kontrol ettiği bir yapı değil.

Bu VÇ’lerde güven zinciri var ve hep bir tarafa doğru. Bitcoin gibi blokzinciri sistemleri ise “trustless” yani onlar güven şartı aramıyor. Bu sistemler, emniyet, yani security temelli bir yaklaşımla, kuvvetli şifreleme teknikleri kullanarak bir noktadan diğerine asset (değer) yollayabiliyorlar.

Blokzincirileri sadece finansal enstrümanlar için kullanılmıyor. Başka pek çok uygulama alanı var. Uluslararası mal taşımacılığında, tarımda, sağlık alanında, sigortacılıkta ve daha pek çok alanda uygulama alanı var blokzinciri teknolojisinin.

Protokol: Bir seri kuraldan oluşan bir döküman. İki taraf arasında döküman/dosya değiş tokuşunda ya da bilgi değişiminde bu kural setleri hız ve kolaylık sağlar. Aynı zamanda hukuka uygunluk ve fraud’u (hilekarlığı) engellemek de protokoller sayesinde mümkün olmaktadır.