BİLGİSAYAR MÜHENDİSLERİ KURULTAYI

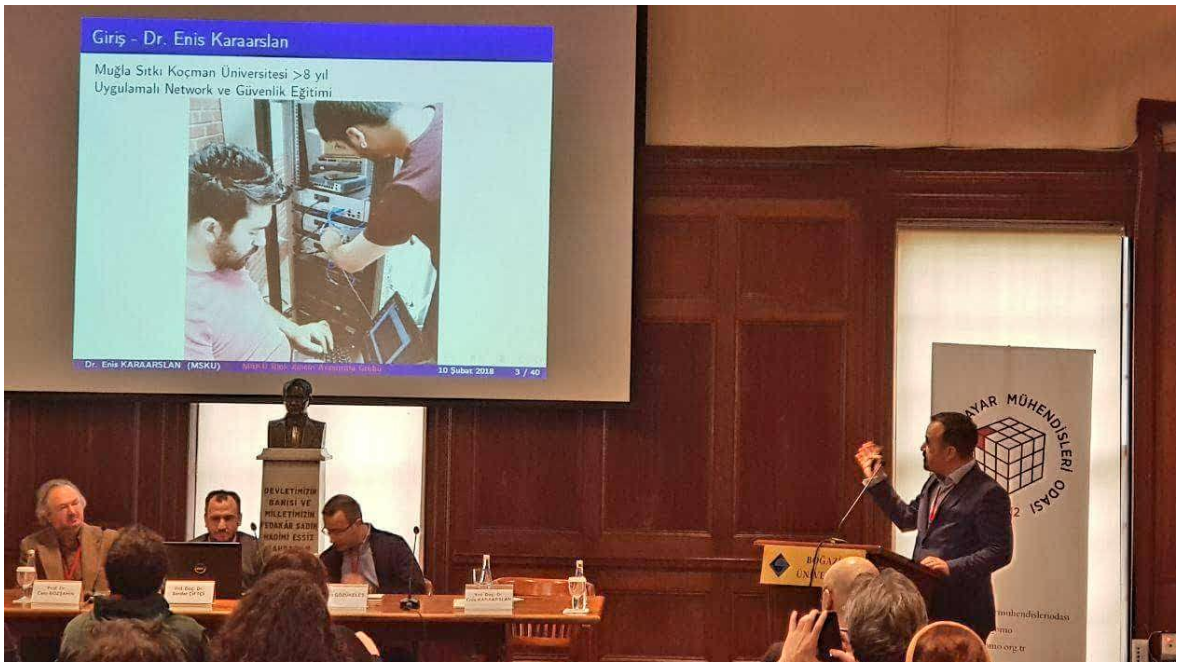
10-11 ŞUBAT 2018, BOĞAZİÇİ ÜNİVERSİTESİ-İSTANBUL

OĞUZ MANAS Oturumu
Güncel Teknolojiler ve Geleceğin Mühendisliği

Yrd. Doç. Dr. Enis KARAARSLAN
Muğla Sıtkı Koçman Üniversitesi Bilgisayar Mühendisliği Bölümü
Blokzinciri Araştırma Grubu

Blokzinciri ve Fırsatlar

"Güncel Teknolojiler ve Geleceğin Mühendisliği" oturumunda blokzinciri teknolojisi üzerine konuşmanın, özellikle de hocamız Oğuz Manas'ın adının verildiği oturumda bulunmanın benim için ayrı bir anlamı var. Oğuz Manas'ın kurucularından olduğu BAUM'a bağlı olan Ege Üniversitesi Kampus Network Yönetim Grubunda (NYG) 10 sene çalıştım. Ağ tasarımı, ağ kurulumu, ağ ve güvenlik yönetimi yaptım. Şu anda Muğla Sıtkı Koçman Üniversitesi Bilgisayar Mühendisliği bölümünde öğretim üyesiyim. Özellikle uygulamalı bilgisayar ağları ve güvenlik eğitiminde bir fark yaratmaya çalışıyorum. Blokzinciri üzerine aktif bir araştırma grubumuz var.



2017 Şubat ayından beridir blokzinciri çalışıyorum. Blokzinciri derken, "bitcoin" değil, madencilik ("mining") de değil. Temel kavramları hızlıca ele alalım. Aslında bütün öğeleri tanıyorduk. Satoshi? O da kim? Belki de konuşmanın sonunda kim olduğunu söylerim. Tuzak kapısı ("trapdoor") fonksiyonları, asimetrik şifreleme, eliptik eğri, sağlama ("hash") fonksiyonları, p2p ağlarını biliyor ve kullanıyorduk. Özellikle p2p ağlarının birçok sorun için çözüm olabileceğini söylüyor ve öğrencilerimizle bu konuda çalışıyorduk.

Herkes blokzinciri konuşuyor, herkes blokzinciri uzmanı. Konuşan kişiye, söylediği bilgiye dikkat etmeli. Biz, açık fikirli insanlarla konuşurken "öğreniyoruz" diyoruz. Ama bazıları bunu, konu hakkında az bilgimiz olduğuna yorabileceğinden, o tür ortamlarda da "biliyoruz" diyoruz.

Blokzinciri, yeni bir felsefe, yeni bir bakış açısı sunuyor. Bu sayede merkezi olmayan sistemler mümkün olabilecek. Aracılar aradan çıkartılacak, özgürlük ve güven vaat eden sistemler geliştirilebilecek. Gerçi bazıları daha çok işin duygusal boyutuna bakıyor; Bitcoin fiyatları gene düşmüş, battık :).

Bitcoin (BTC), ilk başarılı uygulama olduğu için önemli. Bitcoin:

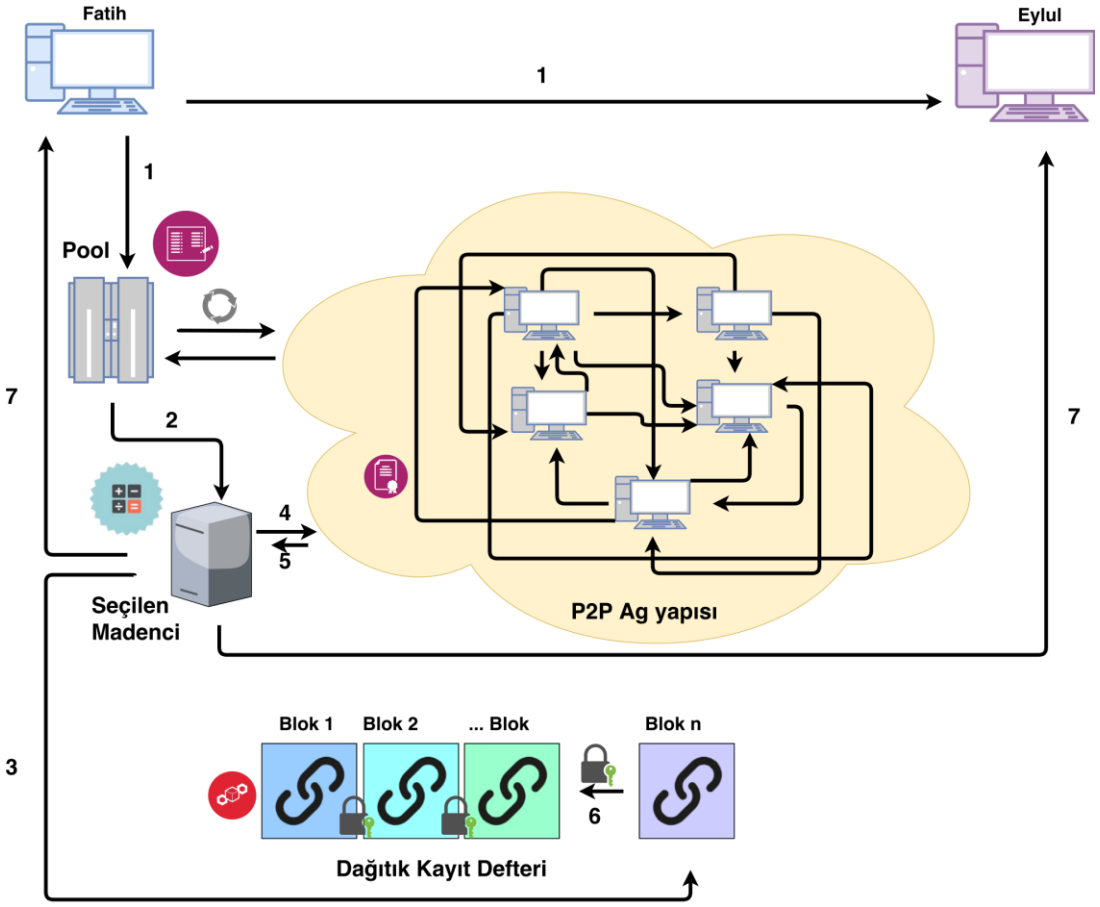
- P2P protokolünü kullanan
- Merkezi olmayan
- Dijital kripto para
- 2009 senesinden beri aktif
- Hiçbir finans kurumunun yönetiminde değil (teoride öyle ama pratikte ?)

"Harvard Business Review" dergisinin Mayıs 2016'daki "Blokzincirinin Finansal Hizmetlerin Ötesinde Etkileri" yazısında, blokzincirinin finansal sektördeki önemi şu cümlelerle belirtiliyor: "Önümüzdeki on yıllık ticareti değiştirme olasılığı en yüksek teknoloji; sosyal ağlar, büyük veri, bulut, robotik ya da yapay zekâ değildir. Blokzinciri'dir."

Sistem Nasıl Çalışıyor?

Blokzinciri sisteminin nasıl çalışacağı, Satoshi'nin 2008 senesindeki yayınlanan teknik yazısında anlatılmıştı. İki bilgisayar arasında yapılması istenen bir işlem, aracı bir kurum tarafından değil, blokzinciri sistemi tarafından onaylanacaktır. Bu sistemde, ağ üzerinde bu işe adanmış ağ düğümleri, işlem havuzu ve sistemin ortak karar ile çalışmasını sağlayan konsensüs protokolünden söz etmek mümkündür. İşlemler onaylandıktan sonra, işlem bilgisi değiştirilmez bir kayıt defterine yazılacak ve bütün ağ düğümlerinde tutulacaktır. Kişilerin altyapıya makinelerini sunmalarını özendirmek için, sistem ödül olarak seçilen düğümlere kripto para vermektedir. Bunun için makinelerin sisteme katkısını ölçmeyi hedefleyen, PoW konsensüs protokolüne dayanan bir süreç (madencilik) gerekmektedir. Madencilik süreci çok fazla elektrik harcanmasına yol açmaktadır. Bu çalışma şeklinin tek yol olmadığını, farklı konsensüs ve farklı çalışma şekillerinin de mümkün olduğunu hatırlatalım.

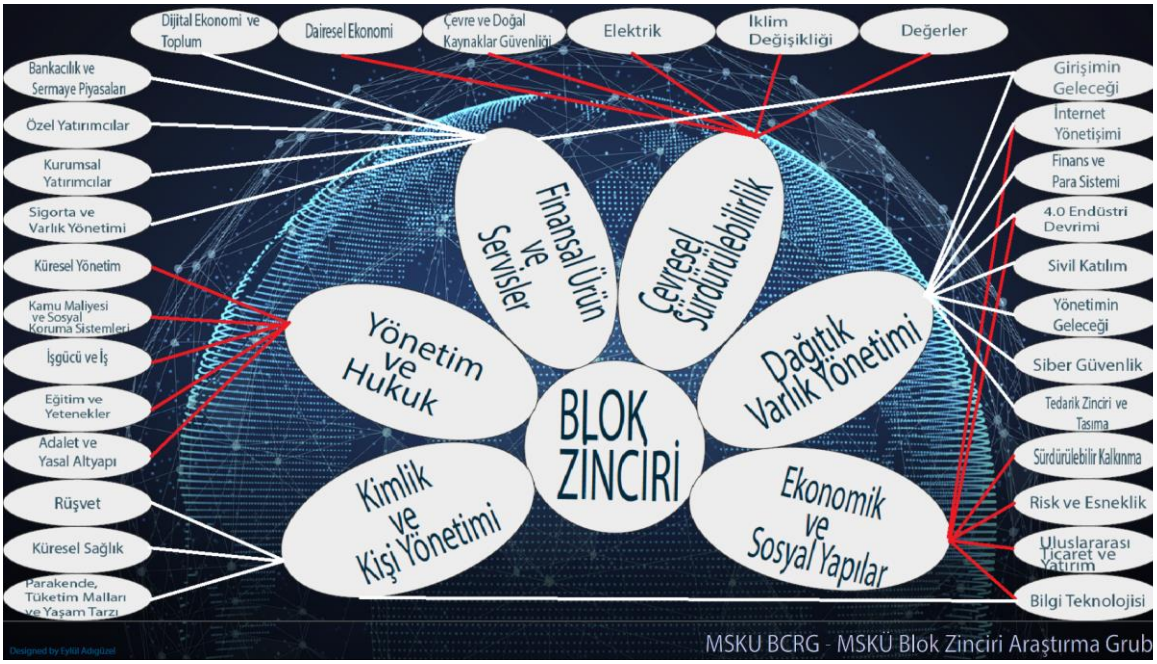
Blokzincirindeki bloklar, kayıt defteri ("ledger") içerisinde birbirine SHA256 gibi sağlama (HASH) fonksiyonları ile bağlıdır. Bu sağlama değerleri, her blokta birbirinin sağlaması alınarak Merkle Ağacı dediğimiz yapıyı oluşturmaktadır. Sistemdeki bir işlemi değiştirmek, o bloğu takip eden zincirdeki diğer blokları da hesaplamayı gerektirir. Sisteme "%51 saldırısı" dediğimiz bir saldırı türü yapılabilir. PoW kullanılıyorsa, saldırganın ağdaki bütün düğümlerin madencilik işlemci gücünün en az %51'ine sahip olması gerektir. Bu saldırının başarıya ulaşma olasılığı çok azdır, kaldı ki bütün işlemler şeffaf bir şekilde sunulduğundan, sistemdeki diğer kişiler saldırının farkına varacaktır.



Blokzinciri sistemleri, merkezi veritabanları ve dağıtık veritabanlarına göre veri bütünlüğü ("data integrity"), kullanılabilirlik ("availability") ve hata toleransı ("fault tolerance") güvenlik servislerini çok daha yüksek başarımlarla sağlayabilmektedir. Mahremiyet ("privacy") amaçlanmamakta, ama sağlanması mümkündür. Gizlilik ("confidentiality") ise düşük seviyede sağlanmaktadır.

Blokzinciri Tabanlı Sistemler

Blokzincirinin günümüzde öncü ve en popüler uygulamaları kripto paralar olsa da aslında birçok uygulama alanı var. Öncelikle bu teknolojinin deneme sürecinde olduğumuzu, şu an ön ürünlerin (prototip) ortaya çıktığını ve henüz tam gelişmiş sistemlerin henüz var olmadığını hatırlatmak gerekiyor. Blokzinciri tabanlı belli başlı projeler olarak günümüzde FinTech diye adlandırdığımız finansa teknoloji uygulanması ve tedarik yönetim sistemlerinden söz etmemiz mümkün. Devrim yaratması beklenen sektörler de aşağıdaki şekildeki gibidir.



Öncelikle belirtelim ki her uygulama blokzinciri teknolojisiyle geliştirilmeye uygun değildir. Uygulamanın aşağıdaki karakteristiklere sahip olması veya ihtiyaç duyması gerekiyor:

- Birden fazla taraf,
- Paylaşılan veri,
- Tarafların birbirine güven (“trust”) ihtiyacı,
- Denetleme, değiştirilemez ve silinemez kayıtlara ihtiyaç.

Blokzinciri tabanlı sistemlerle hedeflenecekler aşağıdaki gibi olmalıdır:

- TAM GÜVEN,
- Tüm Mahremiyet,
- Odağında herhangi birisinin veya kurumun olmaması,
- Tümden merkezi olmayan sistemler,
- P2P işlemler.

Biz siber güvenlik için de bu teknolojinin kullanılabileceğini düşünüyoruz. İnternet'e bağlı olan cihazların sayısının, çeşidinin artması ile her cihaz ele geçirilebilir. Daha akıllı ve farklı çözümlere ihtiyaç bulunmaktadır.

Sonuç

Sonuç olarak da şunları belirtmek gerekiyor. Başka türlü sistemler mümkün. Sistemler henüz olgunlaşmış değil, henüz ön ürün aşamasındayız. Öncü olmak isteyen kurumlar bu teknolojiyi denemeliler.

Bu teknolojinin geliştirmesi ve sanayi işbirliği için üniversiteler önemlidir. Akademideki öğrenciler bu konuya meraklı ve heyecanlılar. Ortak projeler (Tübitak 2209-B ve diğerleri) yapılmalıdır.

Biz Muğla Sıtkı Koçman Üniversitesi **(**MSKÜ) Bilgisayar Mühendisliği NetSecLab - Blokzinciri Çalışma Grubu (MSKU BcRG) olarak blokzinciri teknolojisine dayanan çözümlerin çalışılması ve geliştirilmesi gerektiğini düşünüyoruz. Öğrencilerimizin bu konuda yetişmesini ve çözümler sunmasını destekliyoruz.

MSKÜ Blokzinciri Araştırma Grubu 2017 Haziran ayında kuruldu. Grubumuz dinamik bir üye sayısına sahip. Konuları tartışıyor ve çözüm önerileri üretiyoruz. Aşağıdaki fotoğrafta, bir öğrencim diğer grup üyelerine blokzinciri sisteminin nasıl çalıştığını anlatıyor. Birçok etkinlikte sunum yapıp bu konuda bilinçlendirme çalışmalarına katkıda bulunduk**.** Türkçe içerik üretiyor ve wiki sayfamızdan paylaşıyoruz. MSKÜ blokzinciri araştırma grubu sayfasına http://wiki.netseclab.mu.edu.tr/index.php?title=MSKU_BcRG adresinden ulaşabilirsiniz.

İznizle üniversite eğitimine dair birkaç düşüncemi dile getirmek istiyorum. Üniversite sadece bilgilerin verildiği değil, aslında fikirlerin tartışıldığı yer olmalıdır. Bunu birçok düşünür, bilim insanı da belirmiştir. Cahit Arf der ki

"Biz öğrenciye ne öğreteceğimizi tam olarak bilmiyoruz. Daha doğrusu emin değiliz.
Eğer öğreteceğimiz her şeyden emin olsaydık, o zaman orası üniversite olmazdı.
Üniversite, tartışarak gerçeklerin arandığı bir kurumdur."

Tek ihtiyacımız, öğrencilerde oluşturulacak:

- Hayal
- Hedef
- Heyecan
- Tutku

Ortak çalışmalar oluşturulması hedefimiz var. Bir Afrika atasözünde de denildiği gibi,

"*Hızlı gitmek istiyorsan, yalnız git…*
Uzağa gitmek istiyorsan birlikte yürü"

enis.karaarslan@mu.edu.tr