Siber Güvenlik için Blokzinciri Kullanımı

Dr. Enis KARAARSLAN

Muğla Sıtkı Koçman Üniversitesi
Bilgisayar Mühendisliği Bölümü
BcRG - Blokzinciri Araştırma Grubu

enis.karaarslan@mu.edu.tr

2 Nisan 2018

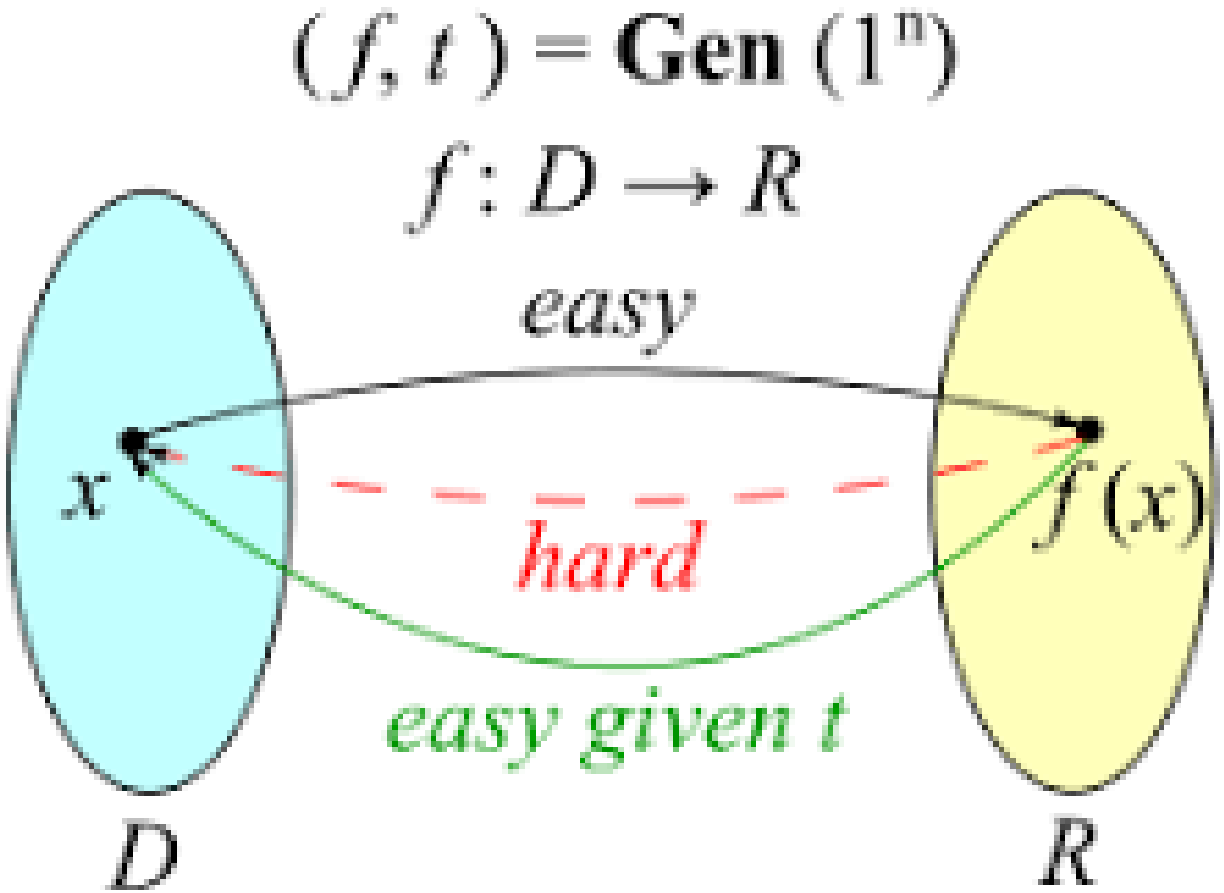
İçerik

- Temel Kavramlar
- Blokzinciri Sistemi
- Güvenlik Felsefesi
- Siber Güvenlik Çözümleri

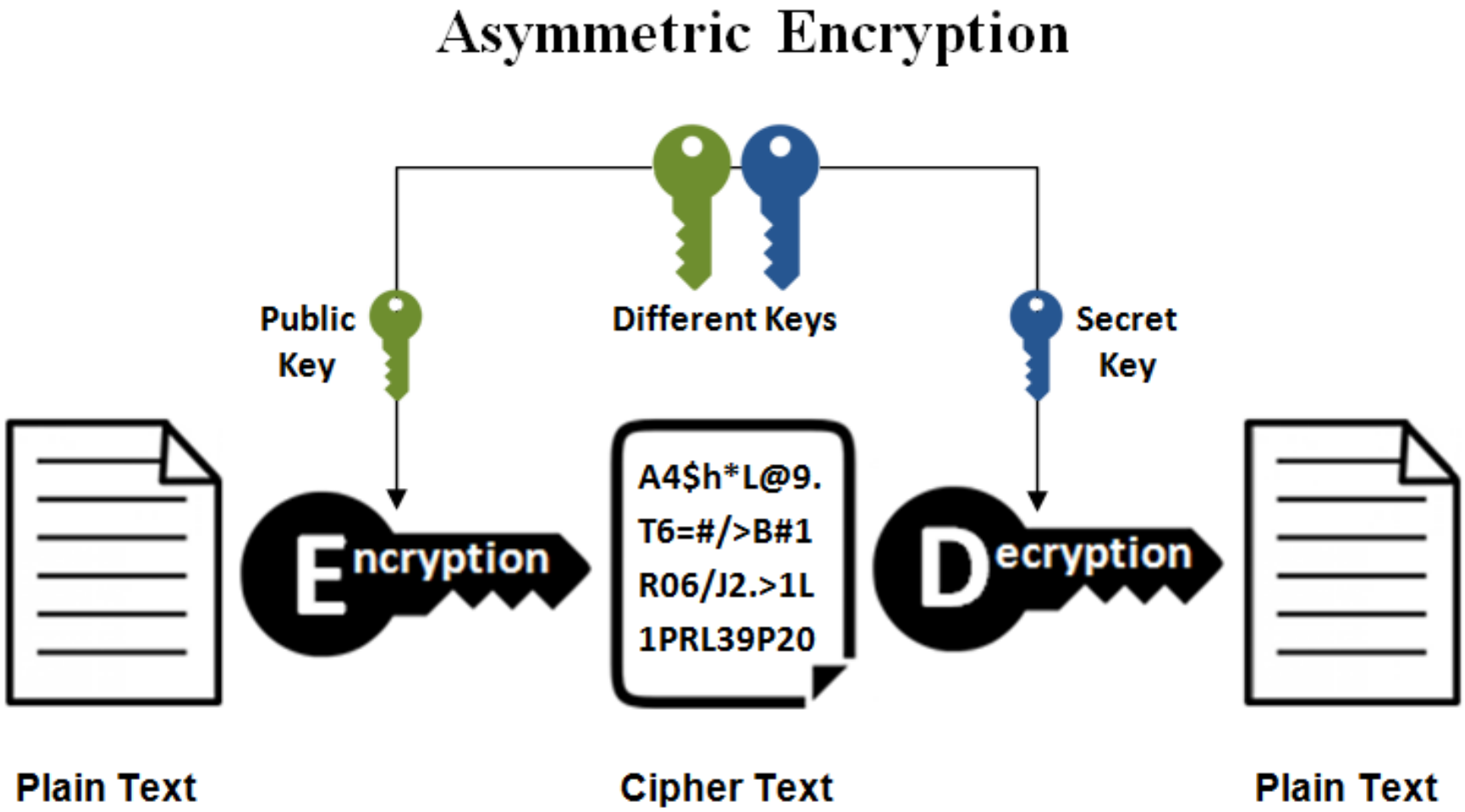
Temel Kavramlar

Aslında bütün öğeleri tanıyorduk -Satoshi kim?

Trapdoor Fonksiyonu

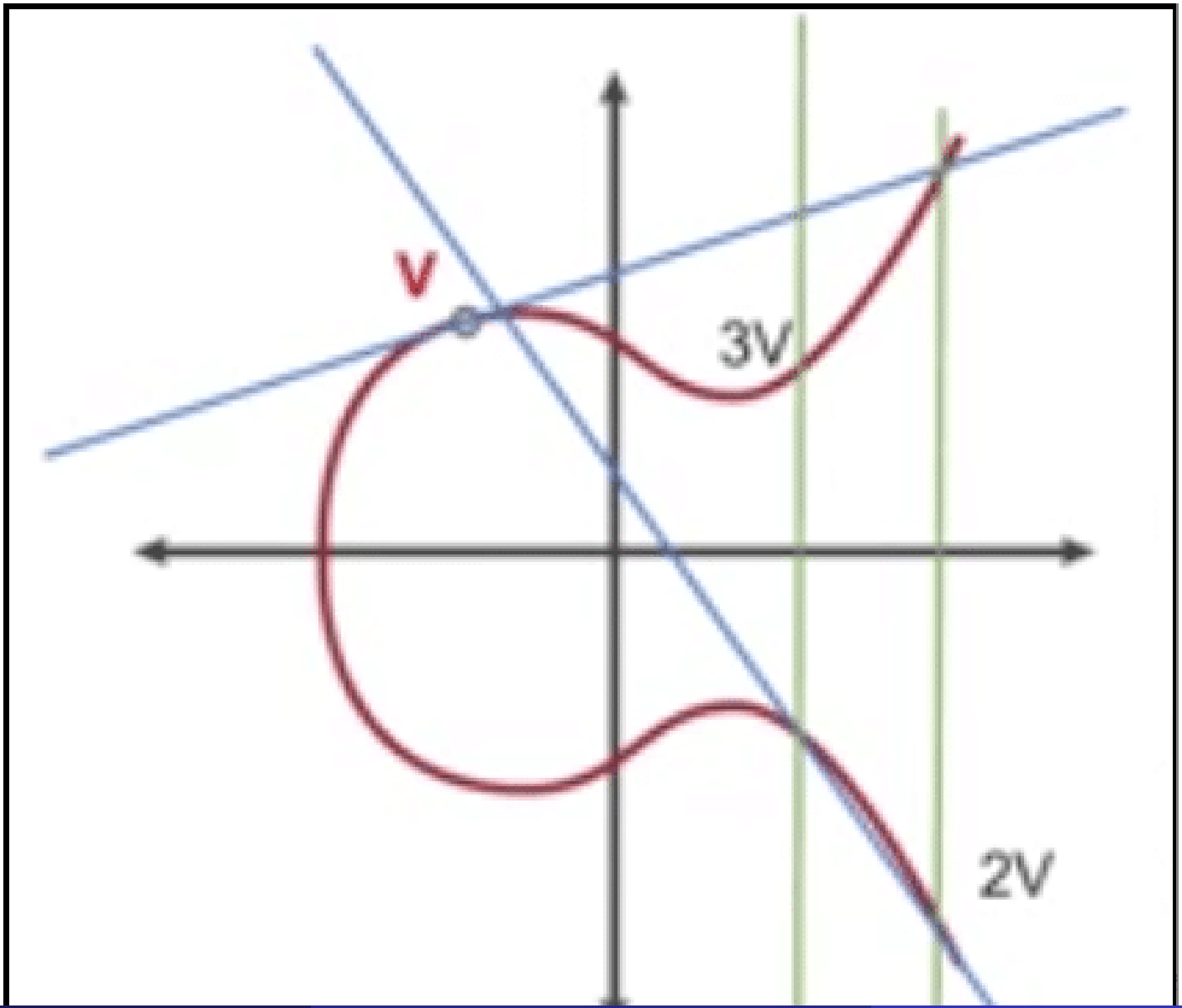


Asimetrik Şifreleme

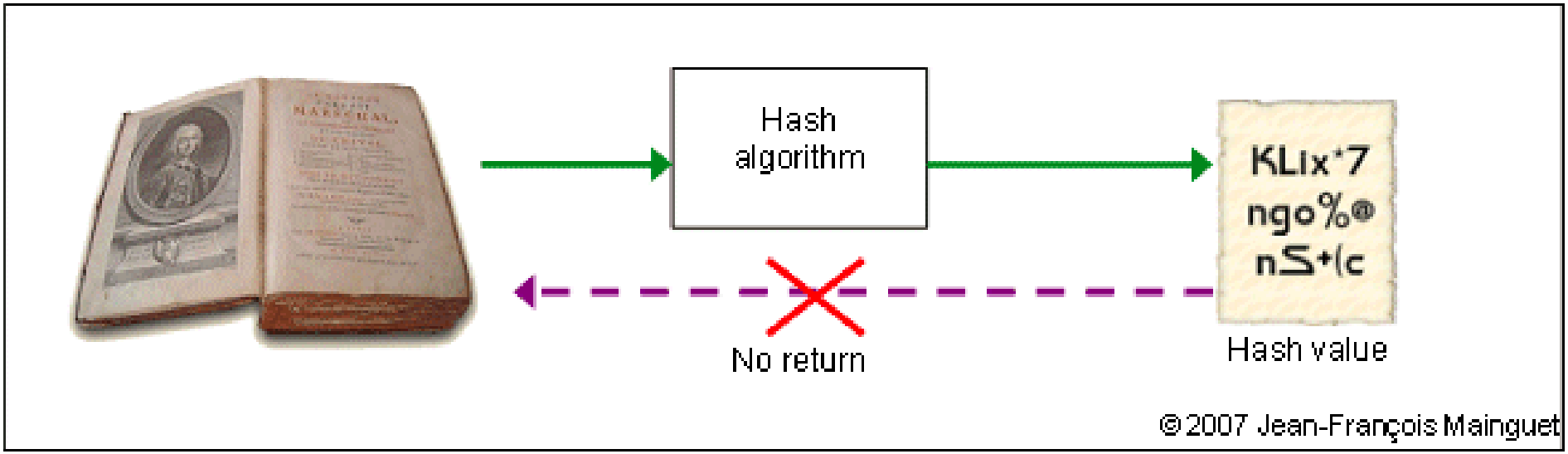


Eliptik Eğri - Eliptic Curve

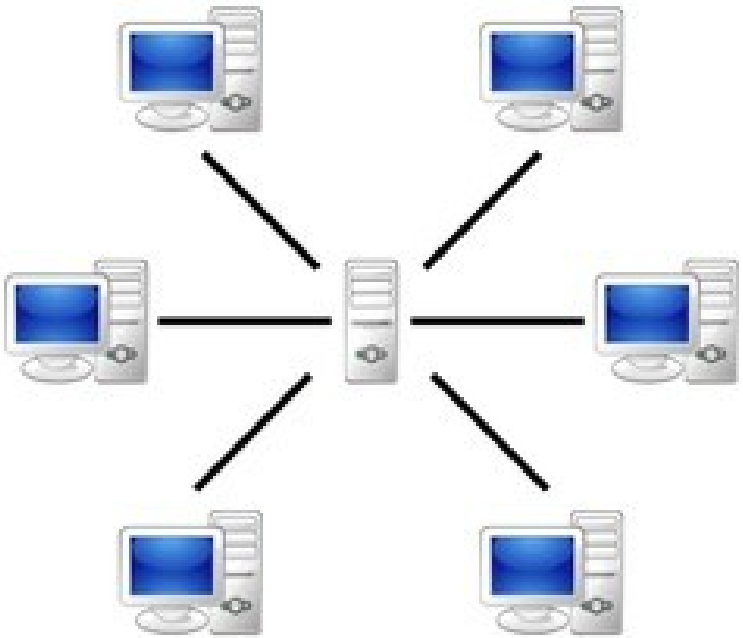
Bitcoin ve Ethereum Eliptik şifreleme kullanıyorlar



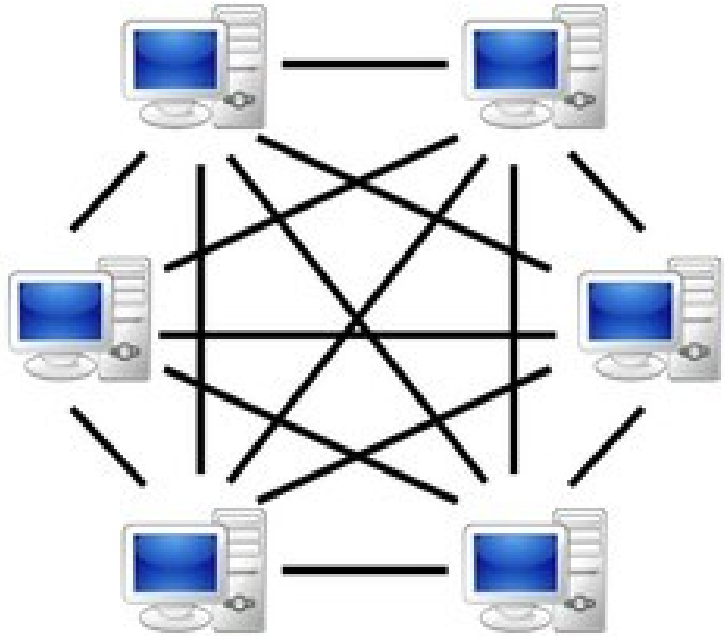
HASH


Hash
algorithm
KLIx*7
ngo%@
nS+(c
No return
Hash value
©2007 Jean-François Mainguet

P2P



Server-based



P2P-network

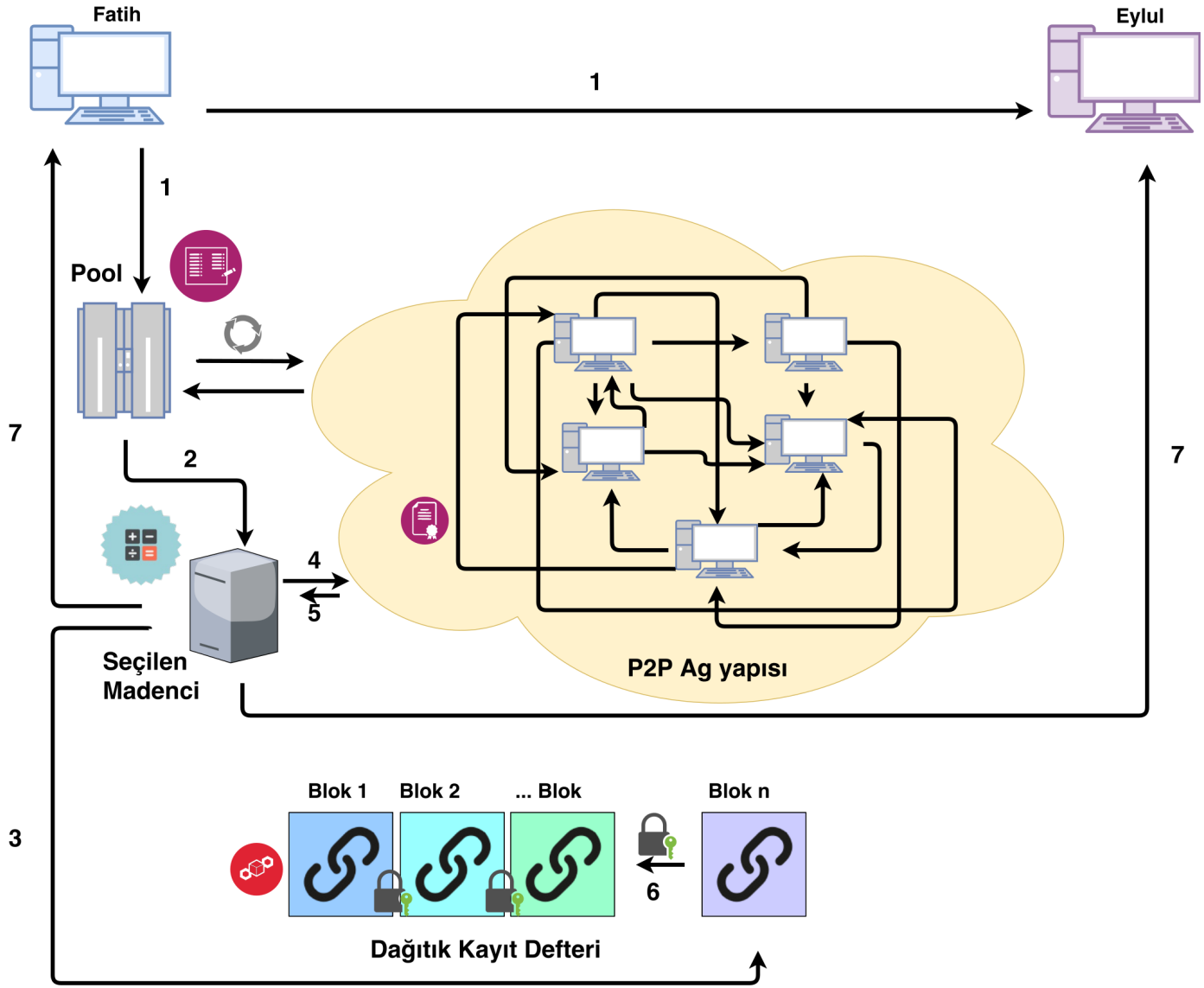
Yeni bir felsefe

Merkezi olmayan sistemler

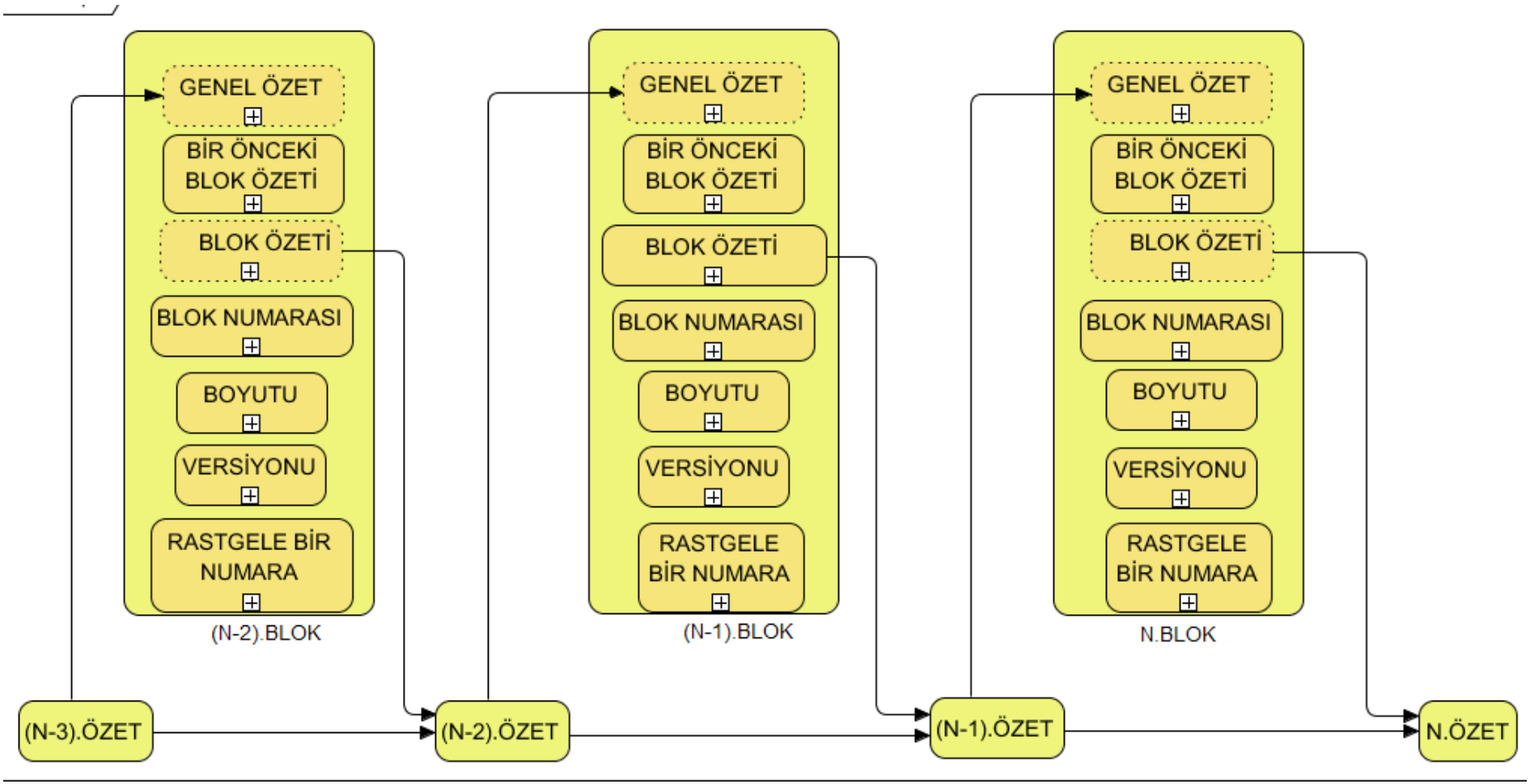
- Aracıların aradan çıkartıldığı (ya da aracıların farkında olmadığımız) sistemler...
- Özgürlük?
- Güven?

Ya da Tamamen Duygusal

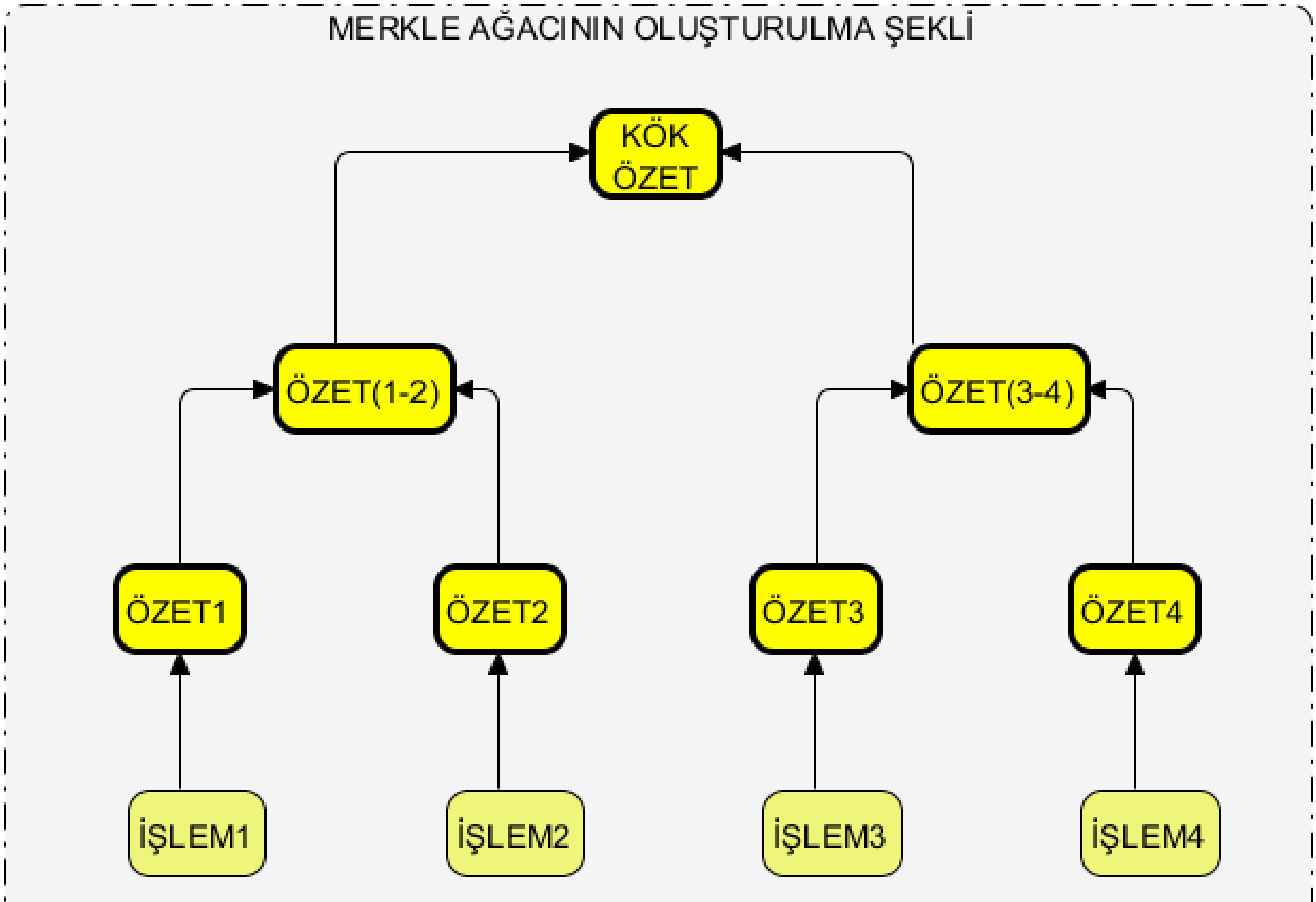
Sistemin Çalışması



Sistemin Çalışması



Sistemin Çalışması



Her uygulamaya blok zinciri teknolojisi uygulanabilir mi?

Her uygulama blok zinciri teknolojisi ile geliştirilmeye uygun değil.
Aşağıdaki karakteristiklere sahip olması veya ihtiyaç duyması gerekiyor

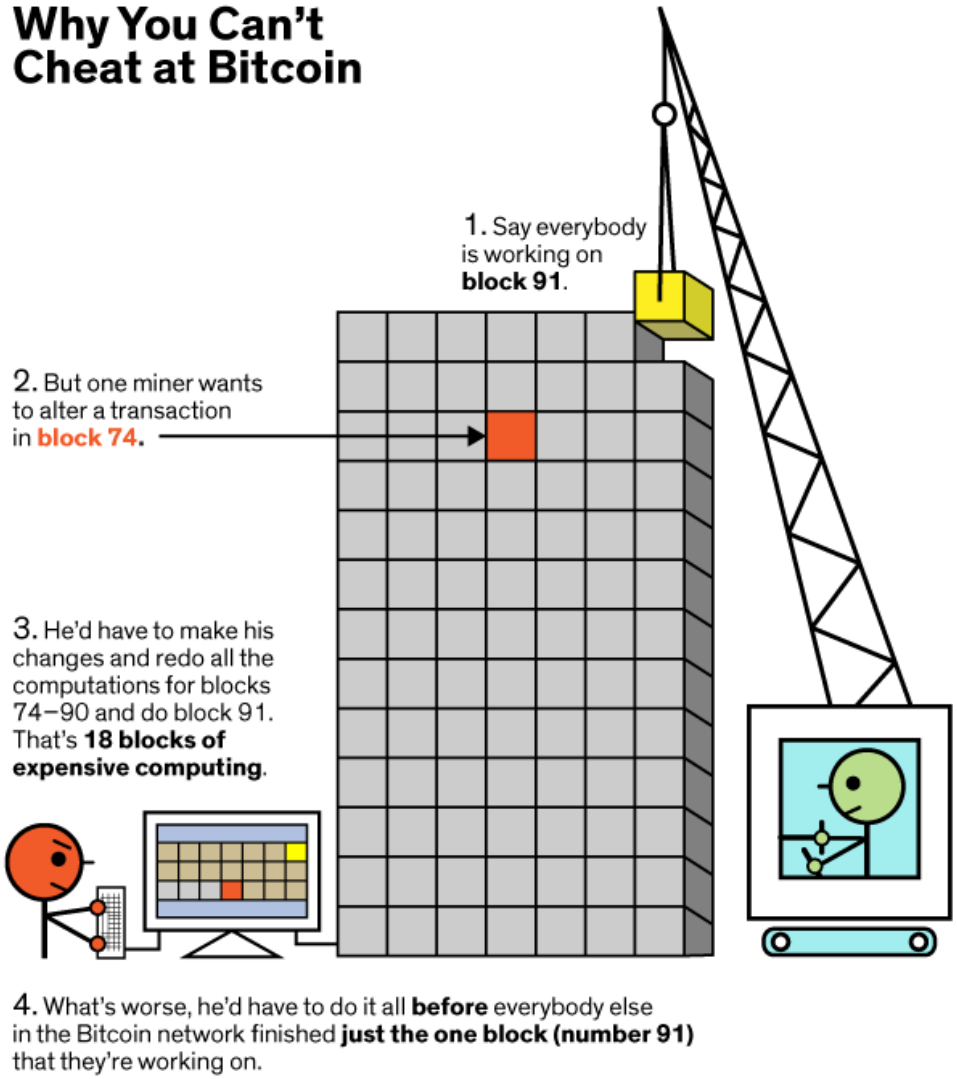
- Birden fazla taraf
- Paylaşılan veri
- Düşük güven
- Denetleme ihtiyacı: değiştirilemez ve silinemez kayıtlar

Sistemin Güvenilirliği

Sistemin Güvenilirliği

- Hash: Örn (SHA256) ile bir önceki bloğa bağlı
- Sistemdeki bir işlemi değiştirmek, zincirdeki tüm blokları da hesaplamayı gerektirir
- %51 Saldırısı: PoW kullanılıyorsa, ağdaki bütün düğümlerin madencilik işlemci gücünün en az %51'ine sahip olması gerek

Sistemin Güvenilirliği



Güvenlik Servisleri

Blokzinciri ile **değiştirilemez kayıtların** oluşturulması en önemli özelliktir.
Bu yapı da **GÜVEN (trust)** oluşturmak için kullanılmaktadır.
Birbirine güvenmeyen tarafların, güvenecekleri işlemlerin yapılması sağlanabilmektedir.

Güvenlik Servisleri

- Veri bütünlüğü (data integrity)
- Kullanılabilirlik (availability)
- Hata toleransı (fault tolerance)

Mahremiyet (privacy)- Amaç mahremiyet değil ama sağlanması mümkün.

Güvenlik Servislerinin Kıyaslaması

	Blok Zinciri	Merkezi Veritabanı	Dağıtık Veritabanı
Bütünlük	Yüksek	Orta	Orta
Kullanılabilirlik	Yüksek	Düşük	Orta
Hata Toleransı	Yüksek	Düşük	Yüksek
Gizlilik	Düşük	Yüksek	Orta

Güvenlik Felsefesi

Güvenlik üzerine biraz düşünelim

Güvenlik Felsefesi

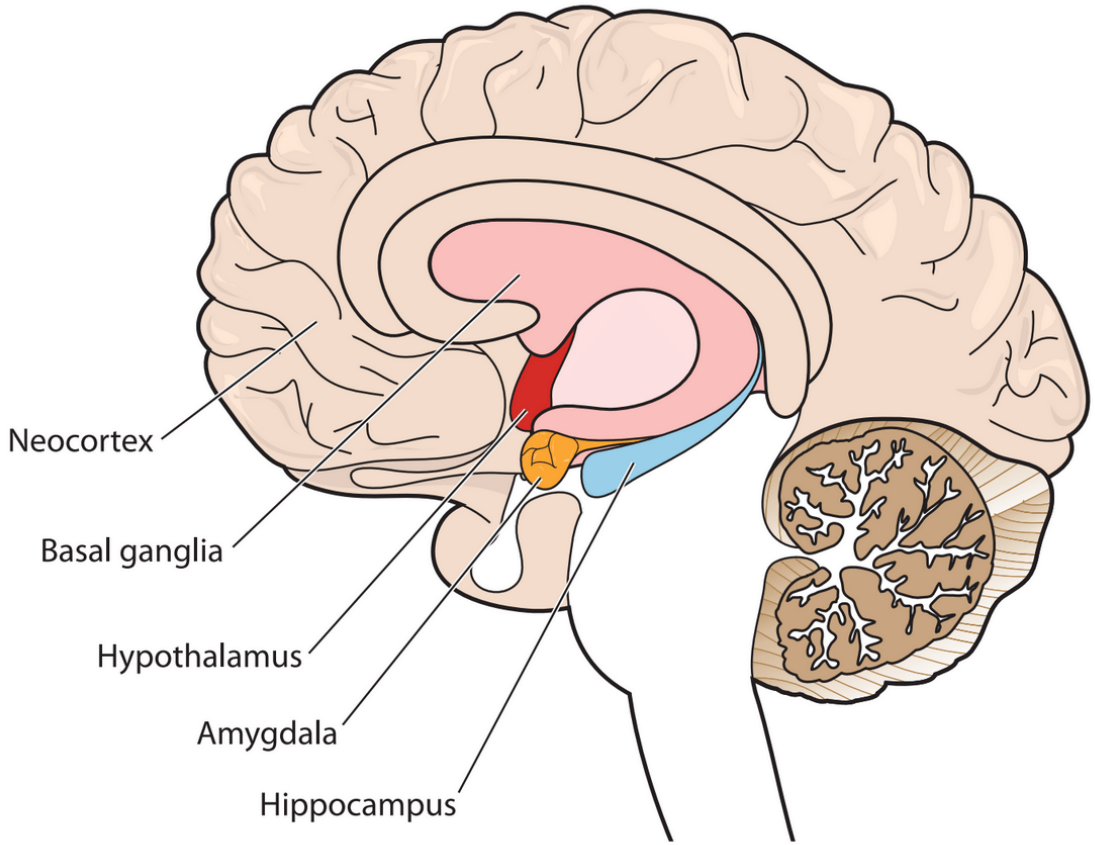
Güvenlik bir ürün değil, bir SÜREÇTİR!
(Bruce Schneier)

Güvenlik Önlemleri ve Risk

Güvenliği sağlamak aslında **"risk"**i değerlendirip güvenlik önlemi alıp almamakla ilgilidir ...
Ne kadar risk alıyoruz?

Beyin – Amygdala x NeoCortex

Risk analizinde beynin hangi kısmını kullanıyoruz?
İlkel "Amygdala" mı
Akıllı ve analitik olan "Neocortex" mi?



İhtiyacımız olan

İhtiyacımız olan,
Karar/önlem alabilmek için sistemleri takip etmek
Sistemde olan bitenlere dair ayrıntılı kayıtlar.

Siber Güvenlik

Siber Güvenlik

Her şeyin birbirine bağlı (connected) olmaya başladığı bir dünyada Siber Güvenlik çok daha önem kazanmaktadır.
Her cihaz ele geçirilebilir
Daha akıllı ve farklı çözümlere olan ihtiyaç

Bütün Cihazlarınız Ele Geçirilebilir

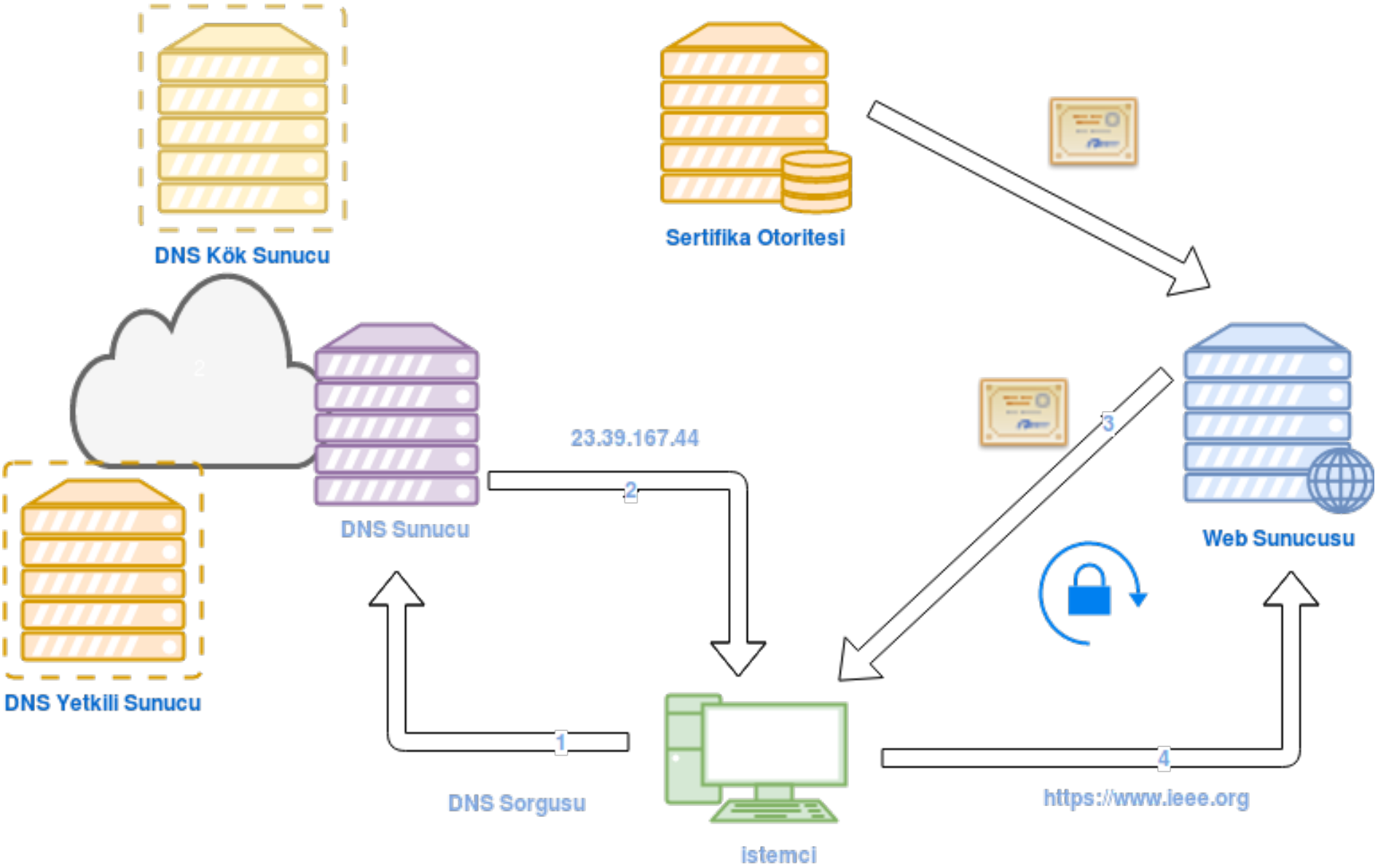
Bütün derken?

- Vücuda takılan cihazlar
- Araba
- Uçak
- Akıllı evler
- IoT ile herşey ...

Siber Savunma: Yeni bir siber savunma yaklaşımı modeli

- **Değiştirilemez kayıtlar** oluşturmak
- Sistemde zayıflık takibi yerine **değişikliklerin izleme**nin etkinliği
- İletişim altyapısına saldırı yapıldığında; **iletişimin devamını sağlayabilen altyapı**lar kurulabilir

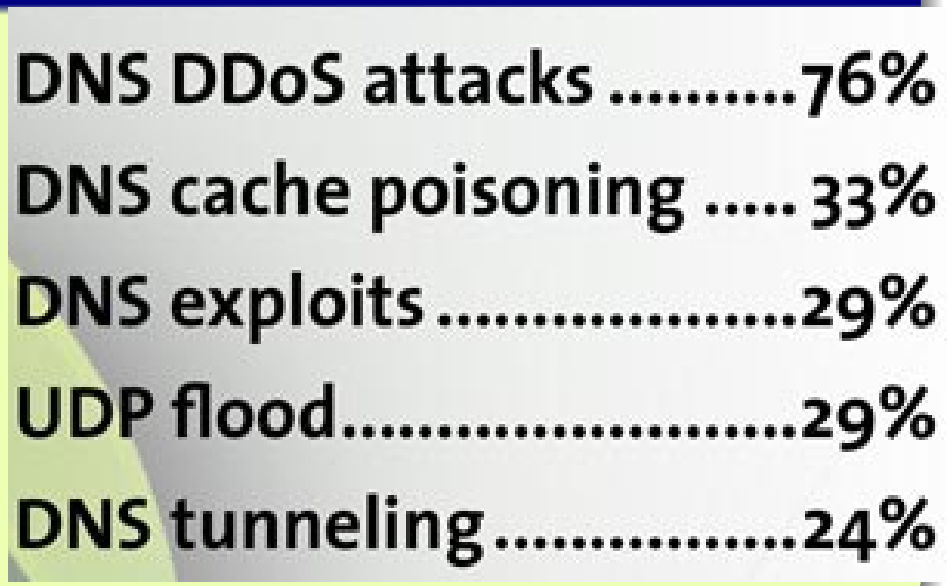
Merkezi Internet: DNS ve Sertifika Otoritesi



Saldırı: Senaryolar

Saldırılar:

- DNS Saldırıları
- Sertifika Otoritesi Sorunları
- Sistemdeki izlerin (log) silinmesi



Çözüm: Merkezi olmayan (Decentralized) Internet

Blokzinciri tabanlı internet:

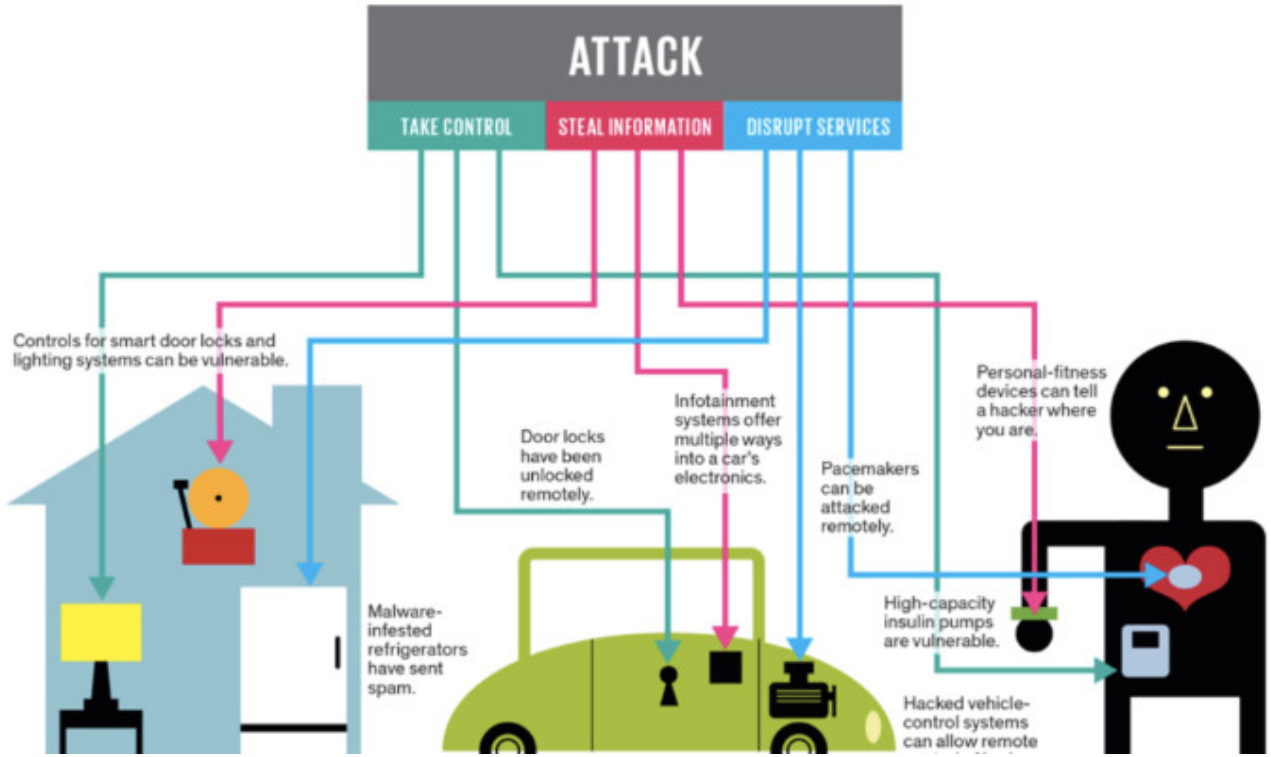
- Özgür, güvenli ve dağıtık bir DNS çözümü (DNSChain)
- Anahtar dağıtımı (PKI) ile sertifika otoritesi
- Bulut Entegrasyonu

Güvenliğinin sağlanmasının o kadar kolay olmadığı çeşitli sistemler

- **Nesnelerin interneti (IoT)** ile birçok kısıtlı bellekli, kısıtlı işlemcili (standartlar oturmadı)
- **Ağ iletişim cihazları**: Bilgisayar ve iletişim ağlarını ayakta tutan cihazlar
- Ağa bağlı herhangi diğer sistemler (yazıcı, kamera vb)

Saldırı Senaryoları

- Cihazların konfigürasyonlarının değiştirilmesi
- Cihazların Aygıt yazılımlarının (firmware) değiştirilmesi
- Sistemdeki izlerin (log) silinmesi



IoT cihazları ile saldırılar

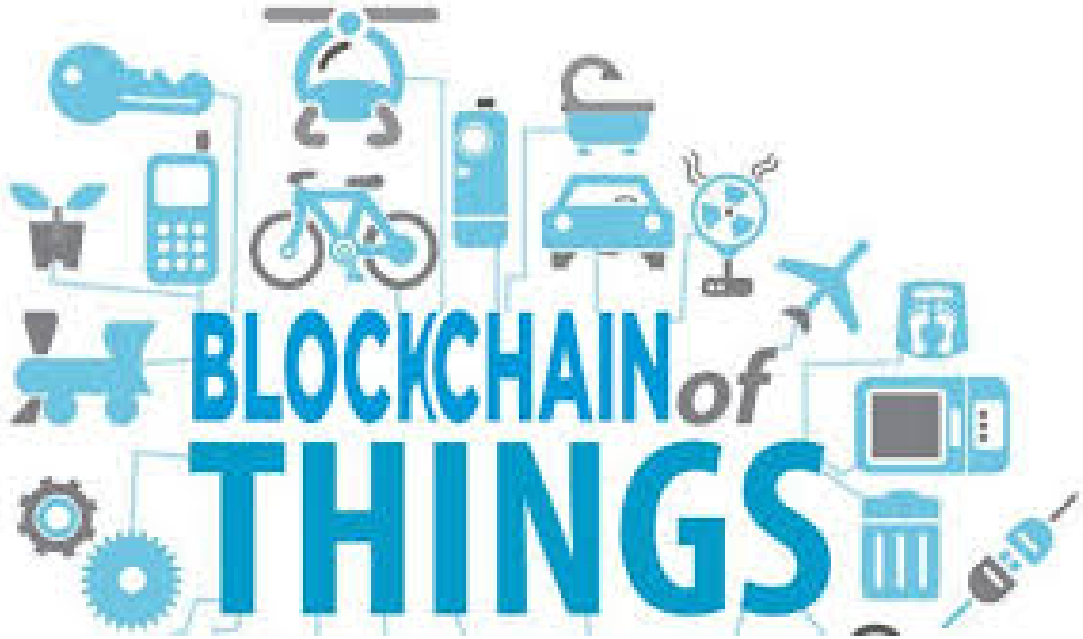
Çözüm: Denetim Sistemleri

- Aygıt konfigürasyonunun takibi
- Aygıt yazılımlarının (firmware) takibi
- Log kayıtlarının saklanması

IoT: IoT Cihazlarının Yönetimi

Yapılabileceklere örnekler:

- IoT cihazlarının davranışlarını belirleyen kodlar
- Açık anahtarlı altyapı ile saldırganların yönetim sistemini kontrol altına almasının önüne geçme
- PoW yerine farklı konsensus protokolleri (Örn: dağıtık güven yöntemi)



Mahremiyet: Elektronik Sağlık Kayıtlarına Erişim Denetimi

- Hastaların, geniş kapsamlı ve değiştirilemez bir sağlık kaydına sahip olması
- Mahremiyet gözetilerek bu sistemin gerçekleştirilmesi
- Bu kayda farklı sağlık kurumlarından kolaylıkla erişebilmesi
- Kayda kimlerin erişebileceğinin hasta tarafından izine bağlı olması

Siber Güvenlik Modeli

Blokzinciri tabanlı siber güvenlik modeli ile yapılabilecekler:

- Kritik verinin korunmasında esneklik sağlanması,
- Veriye kimin ulaşacağı bilgisinin modellenerek, erişim yetkilendirilmesinin sağlanması,
- Erişim ve yapılan işlem bilgisinin emniyetli bir şekilde tutulması,
- Tutulan her bilginin daha sonra denetlenebilir ve sorgulanabilir hale getirilmesi

Dosya Takibi

Bir gizlilik dereceli evrakın yaratıldığını andan itibaren yaşam döngüsü kayıt altına almak

- Kimler tarafından çıktı alındığını
- Hangi bilgisayarın hangi diskine kayıt edildiğini
- Kimin tarafından hangi harici port üzerinden taşınabilir belleğe aktarıldığı sorgulatabilmek

Geliştirilecek Sistemlerin Başarımı

- Tasarım ve Gerçeklenme Başarısına
- Hıza
- Ölçeklenebilirliğine
- Yeni Yaklaşımlar oluşturup oluşturmamıza bağlı ...

Diğer Teknolojilerle Birlikte Kullanımı

- Yapay Zeka (AI)
- Yazılım Tanımlı Ağlar (SDN)

Sonuçlar

Sonuçlar

Blok zinciri ile

- Güven (Trust) sağlayan sistemler
- Güvenlik servislerini birleştiren bir yapı kurulabilir

Sonuçlar

Blok zinciri tabanlı siber güvenlik sistemleri

- IoT, akıllı şehirler ve bilgisayar ağlarının siber güvenliği için ve kişisel verilerin korunmasında kullanımına dair etkin çözümler mümkün
- Ele geçirilmesi diğer çözümlere göre daha zor (%51 saldırısı ve diğerleri)

Sonuçlar (devam)

MSKÜ Blokzinciri Araştırma Grubunda blokzinciri teknolojisine dayanan siber güvenlik modeli ve farklı sektörlere yönelik çözümler üzerine çalışıyoruz.

MSKÜ Blokzinciri Araştırma Grubu

Ortak Çalışma Hedefi

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

Afrika Atasözü

Dinlediğiniz için teşekkürler...

Dr. Enis Karaarslan : enis.karaarslan@mu.edu.tr

MSKÜ Blok Zinciri Araştırma Grubu-
http://wiki.netseclab.mu.edu.tr/index.php?title=MSKU_BcRG