WORLD ENERGY COUNCIL | TURKEY TÜRK MİLLİ KOMİTESİ

Enerji Sektöründe Kayıt Zinciri

Can ARSLAN

Ankara, 24/11/2017

İçerik

1. Kayıt Zinciri
    1. Kayıt Zinciri Mutabakat Mekanizmaları
    2. Kapalı Zincir (Private)
    3. Açık Zincir (Public)
2. Açık Zincir Ölçekleme Problemi
3. Kriptografik Özetleme Fonksiyonları (HASH)
4. İşlemcinin Gücü Adına - Moore’s Kanunu
5. Kriptografi ve İşlemci
6. Özetleme Hızı (Hash Rate) ve Zorluk
7. Açık Kayıt Zinciri Ekonomik Modeli
8. Elektrik Sektöründe Değişim
9. Enerji ve Kayıt Zinciri
    1. Kapalı Zincir Uygulamaları
    2. Açık Zincir ve Modeller

1- Kayıt Zinciri

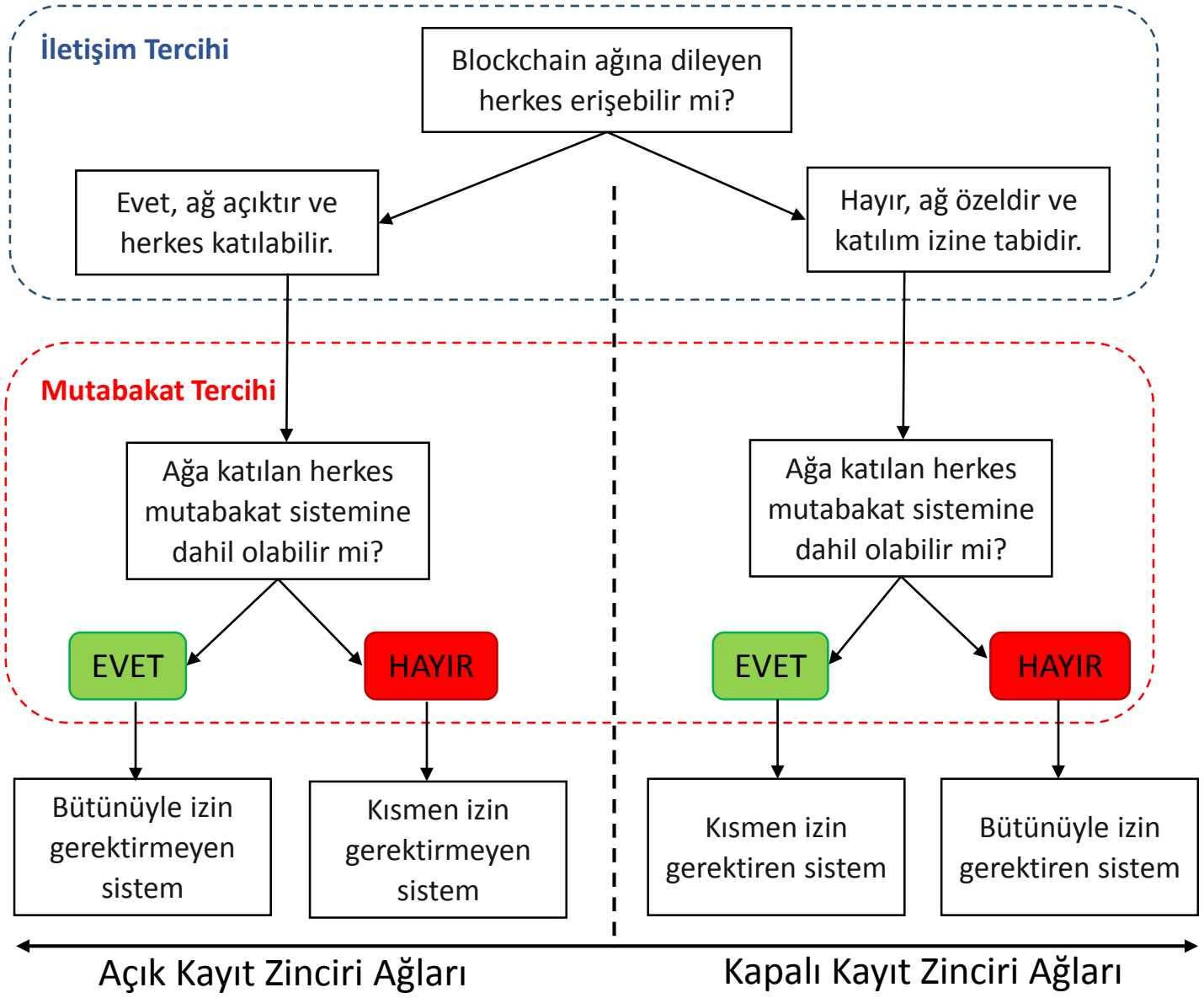
Neden kayıt zinciri?

Neden	Teknoloji
Anonimlik	Şifreleme – Kriptografi
Değiştirilemezlik	Dağıtık Kayıt
İletişim Hızı	Ağ Sunucuları Yazılım Dili

Kayıt Zinciri Tasarımı

1- Açık veya Kapalı Sistem
2- Mutabakat Mekanizması
3- Ölçekleme Sistemi
4- Ekonomik Sistem

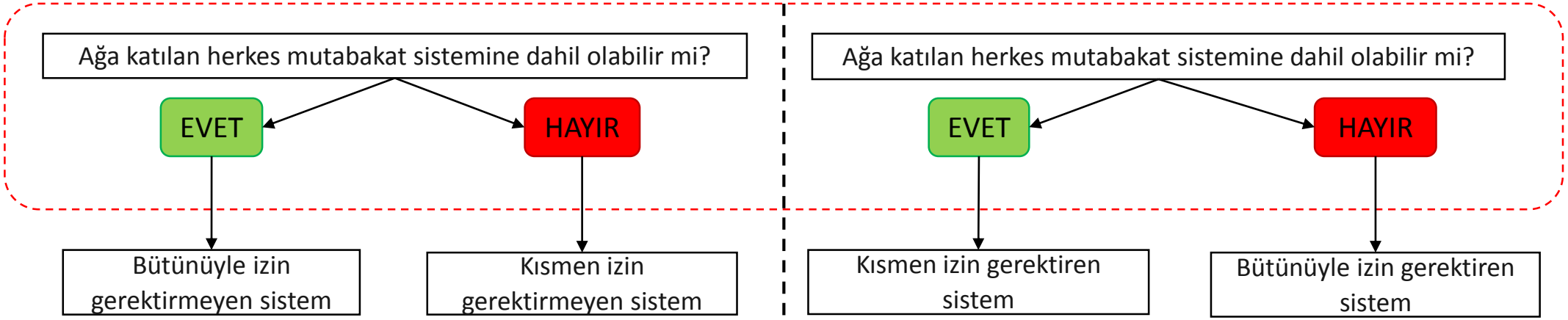
1- Kayıt Zinciri



Usta, Ahmet and Serkan Doğantekin. Blockchain 101. İstanbul: Kapital Medya Hizmetleri A.Ş., 2017.

1.1- Kayıt Zinciri Mutabakat Mekanizmaları

Mutabakat Tercihi



İşin İspatı Algoritması
(Proof of Work)
Bitcoin, Ethereum

Ortaklığın İspatı Algoritması
(Proof of Stake)

Atanmış Ortaklığın İspatı Algoritması
(Delegated Proof of Stake)

Bizans Generalleri Problemi Algoritması
(Practical Byzantine Fault Tolarence)
Hyperledger, Stellar, and Ripple

Bizans Generalleri Problemi Algoritması
(Practical Byzantine Fault Tolarence)

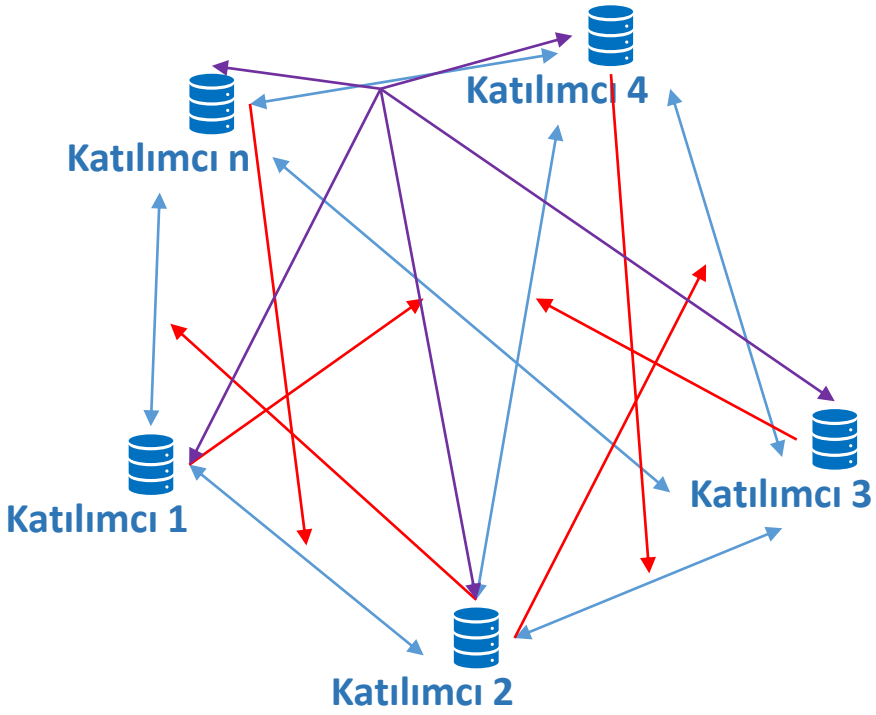
Açık Kayıt Zinciri Ağları ⟷ Kapalı Kayıt Zinciri Ağları

WORLD ENERGY COUNCIL TURKEY TÜRK MİLLİ KOMİTESİ

https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

1.2- Kapalı Zincir

Kısmen İzin Gerektiren Sistem



	Kısmen İzin Gerektiren Sistem	Bütünüyle İzin Gerektiren Sistem
İşlem Adeti	Sınırlı	Sınırlı
Anlık İşlem Sayısı	Sınırsız	Sınırlı
Mutabakat	Tüm Katılımcılar	İzin Verilen Taraflar
Verinin Şifrelenmesi	Tüm Katılımcılar	İzin Verilen Taraflar
Verinin Saklanması	Tüm Katılımcılar	Tüm Katılımcılar
Uygulama Alanları	Ticaret Platformları	Tedarik Zinciri Uygulamaları

Ripple, Hyperledger, Corda

İşlem

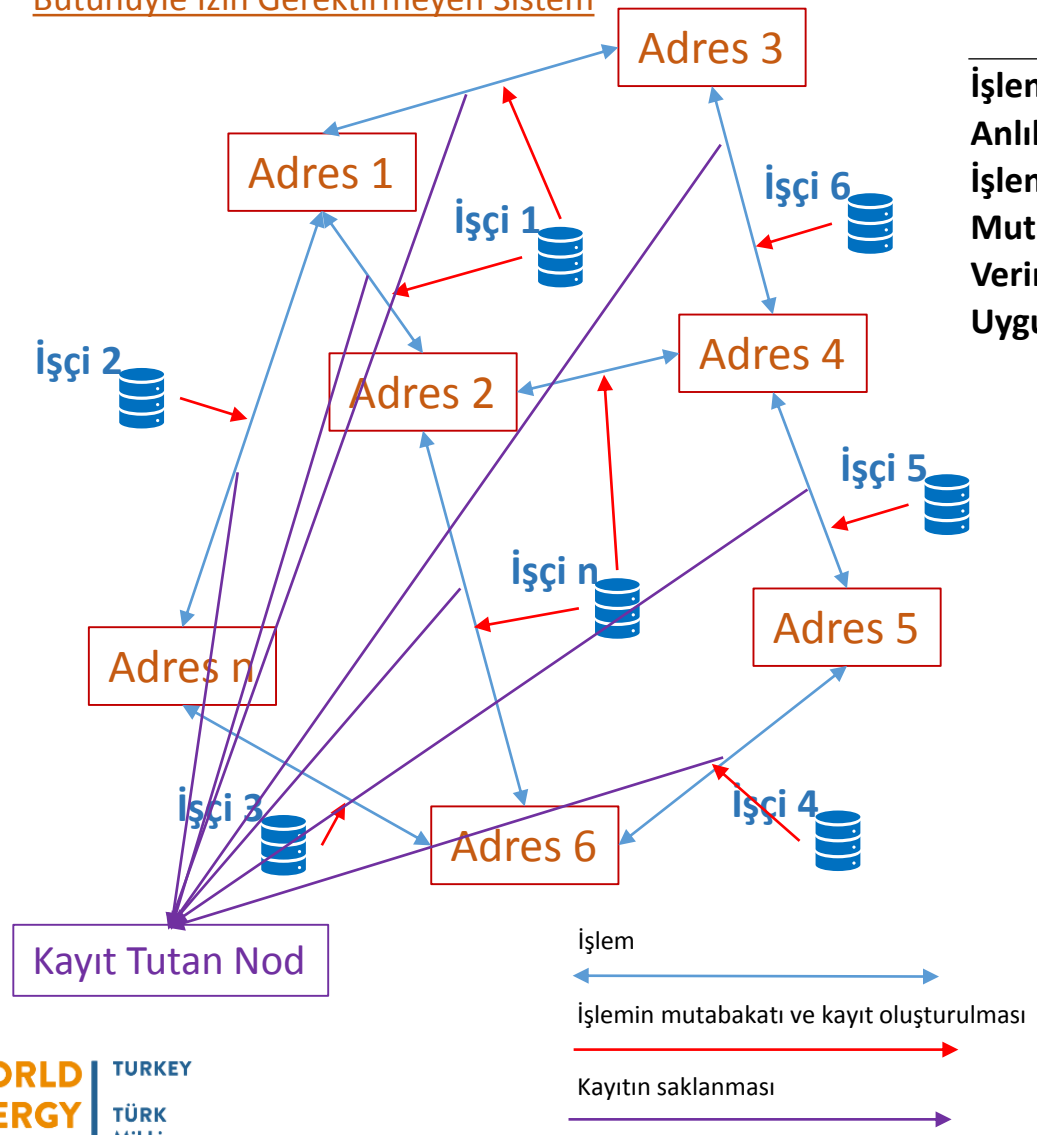
İşlemin mutabakatı ve kayıt oluşturulması

Mutabakat için kaydın saklanması

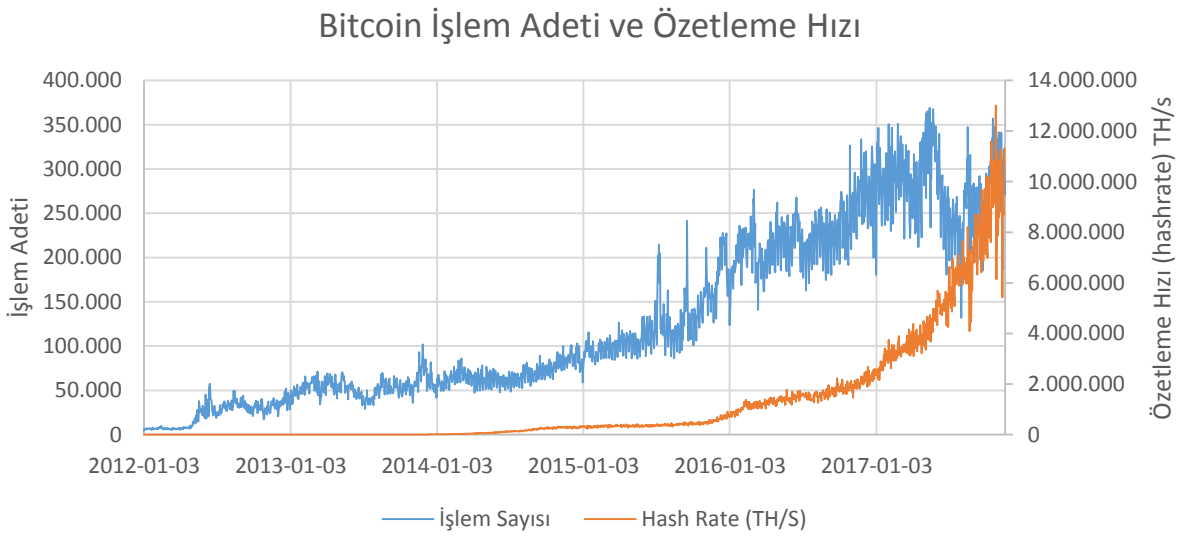
https://wiki.hyperledger.org/groups/requirements/use-case-inventory

1.3- Açık Zincir

Bütünüyle İzin Gerektirmeyen Sistem



	Kısmen İzin Gerektirmeyen Sistem	Bütünüyle İzin Gerektirmeyen Sistem
İşlem Adeti	Sonsuz	Sonsuz
Anlık İşlem Sayısı	Sınırlı	Sınırsız
İşlem Kaydı Oluşturulması	İzin Verilen Taraflar	İsteyen katılımcılar (İşçi Miner)
Mutabakat	İzin Verilen Taraflar	Tüm Katılımcılar
Verinin Saklanması	İzin Verilen Taraflar	İsteyen katılımcılar (Nodlar)
Uygulama Alanları	E-Devlet Uygulamaları	Ödül Mekanizması Olan Sistemler (Bitcoin, Ethereum)

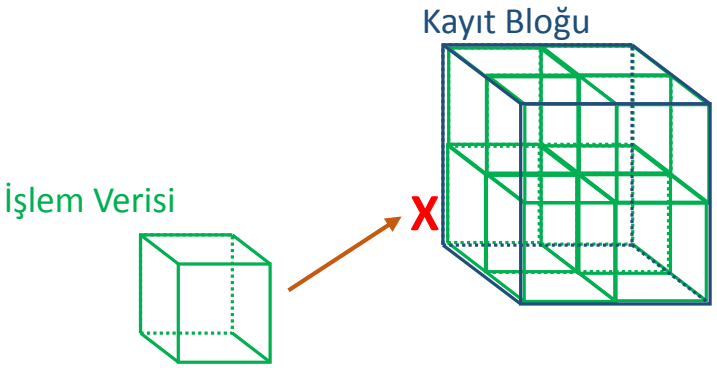


WORLD ENERGY COUNCIL | TURKEY TÜRK MİLLİ KOMİTESİ

2- Açık Zincir İşlem Hızı Ölçekleme Problemi

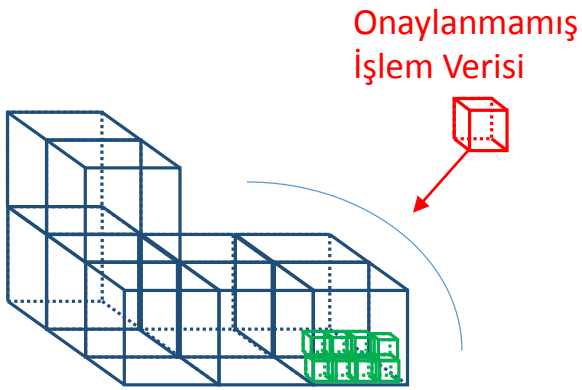
1- İşlem Kaydı Oluşturulması (Bloğa İşleme)

İŞÇİ



2- İşlemin Mutabakatı

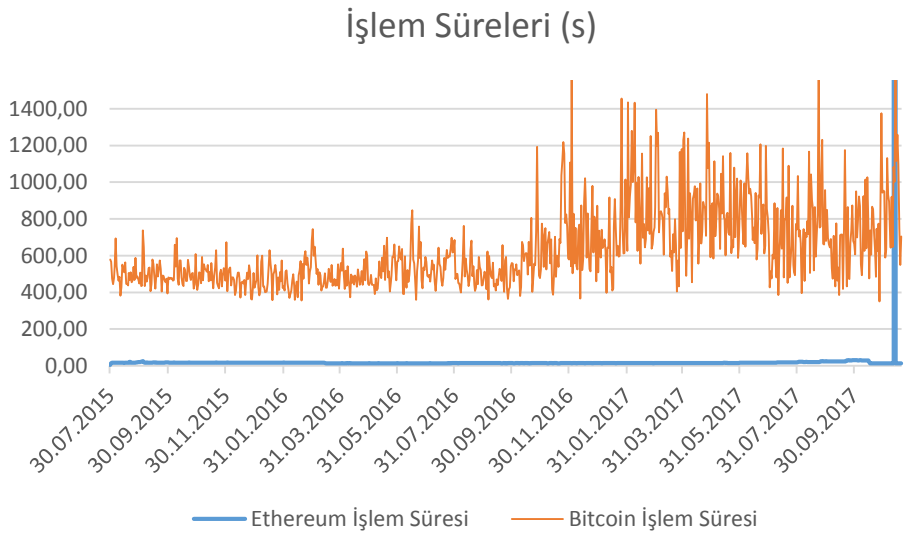
NOD



Çözümler:

1- Kayıt bloğunun büyüklüğü

2- Mutabakat Mekanizmasında değişim



WORLD ENERGY COUNCIL | TURKEY TÜRK MİLLİ KOMİTESİ

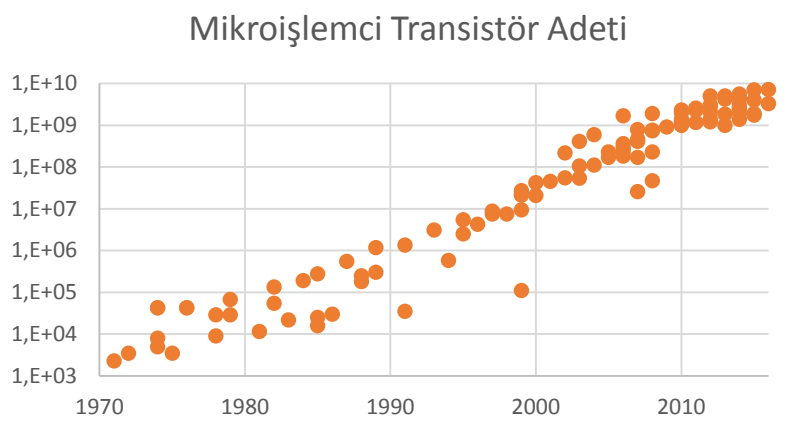
3- Kriptografik Özetleme Fonksiyonları (HASH)

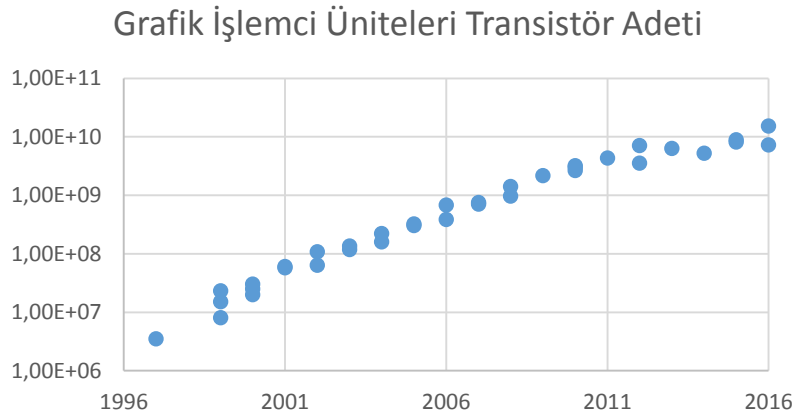
	INPUT	HASH	
A	This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E	H(A)
B	this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C	H(B)

1. **Ön-Görüntüleme Dayanıklılığı (pre-image resistance)**
   - H(A) hash çıkış verisi olsun, A hash giriş verisi. H(A)'dan yolan çıkarak A'yı bulmak mümkün olmayacaktır. Örneğin 128-bit hash fonksiyonu kullandığımızı varsayalım:
   - En kötü ihtimalle 2^128-1 deneme sonra H(A)'dan A'yı çıkarabilirsiniz, ortalama ihtimalde 2^128/2 deneme yapacaktır yani 1.7X10^38 defa denemeniz gerekecek.
2. **Çakışma Dayanıklılığı (Collision resistant)**
   - H(A)'nın H(B)'ye eşit olması mümkün değildir.
   - 128-bit hash 2^128 farklı sonuç verir.
   - Çakışma dayanıklılığını kırmak için %50 şansımız olduğunu düşünürsek sqrt(2^128)=2^64 ihtimal denenmesi lazım.
   - Ön-Görüntüleme dayanıklılığını kırmaktan daha kolay. Hiçbir hash fonksiyonu çakışma dayanıklılığına sahip değildir, sadece bu çakışmayı bulmak çok uzun sürecektir.

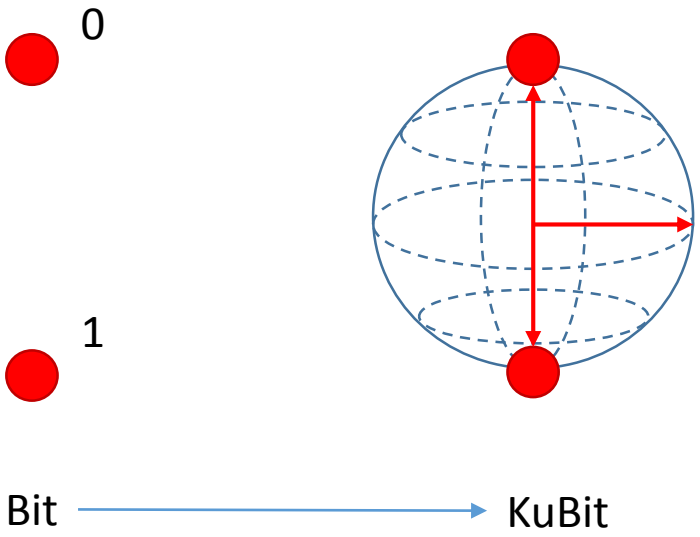
4- İşlemcinin Gücü Adına: Moore’s Kanunu

Transistör sayısı her 18 ayda 2 katına çıkar.

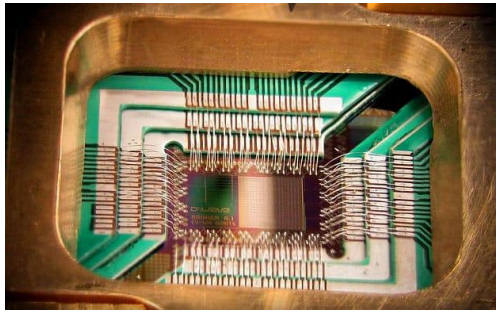




Kuantum Bilgisayarlar



D-Wave Çipi (Google & Nasa)
Normal bilgisayarlardan
100 milyon kat daha hızlı



WORLD ENERGY COUNCIL TURKEY TÜRK MİLLİ KOMİTESİ

https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Transistor_count.html
https://www.research.ibm.com/ibm-q/

5- Kriptografi ve İşlemci Gücü

Genel Kriptografik Özetleme Algoritmalarının Tarih Cetveli																												
Fonksiyon	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Snefru																												
MD2 (128-bit)																												
MD4																												
MD5																												
RIPEMD																												
HAVAL-128																												
SHA-0																												
SHA-1																												
RIPEMD-160																												
SHA-2 family																												
SHA-3 (Keccak)																												

Akran Değerlendirmesi
Güçlü Kabul Edilme
Önemsiz Zayıflık
Zayıflatıldı
Kırıldı
Çakışma Bulundu

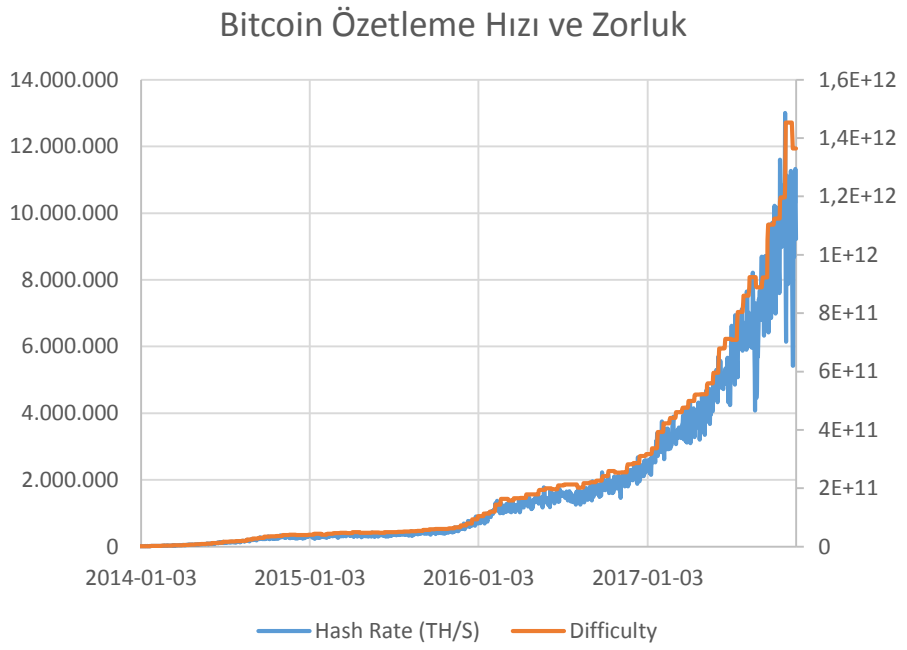
Google ve CWI, 23 Şubat 2017'de SHA-1 fonksiyonununda çakışma buldu!
6,610 İşlemci Yılı

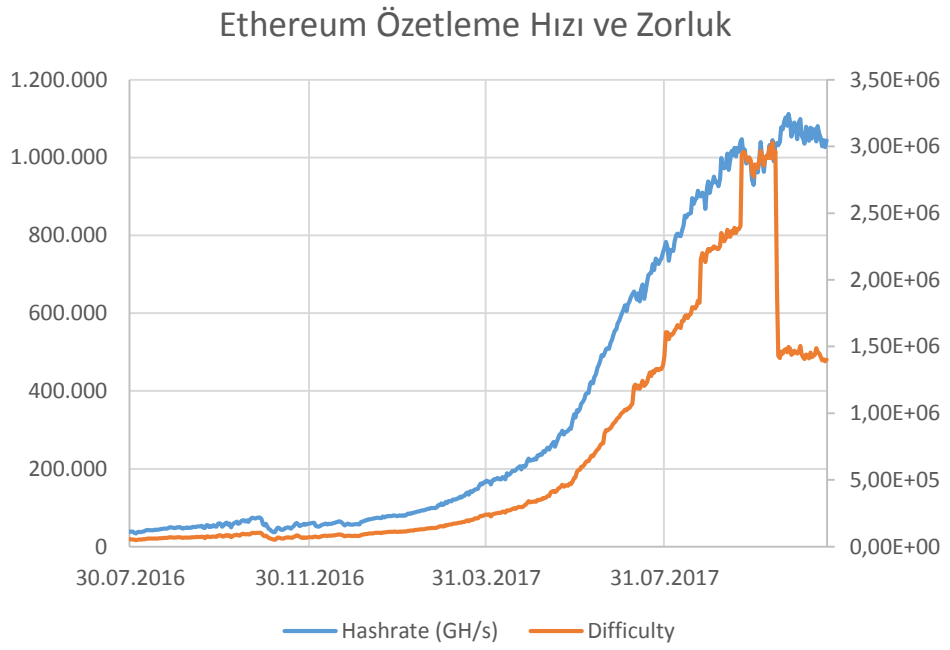
WORLD ENERGY COUNCIL TURKEY TÜRK MİLLİ KOMİTESİ

http://valerieaurora.org/hash.html
https://shattered.io/

6- Özetleme Hızı (Hash Rate) ve Zorluk

Özetleme Hızı: İşçilerin işlemleri onaylamak ve kayıt bloğu üretmek için harcadığı işlemci gücü
Zorluk: İşçilerin Rekabeti, daha fazla işlemci gücü daha yüksek zorluk





Kayıt Zinciri 1.0
Sınırlı blok ve Kesin Blok Büyüklüğü
Dijital para sistemi

Kayıt Zinciri 2.0
Sınırsız blok ve Blok-Veri Yönetimi (Sharding)
Uygulamaların çalıştırıldığı platform

WORLD ENERGY COUNCIL TURKEY TÜRK MİLLİ KOMİTESİ

https://www.quandl.com/data/BCHAIN-Blockchain
https://etherscan.io/charts

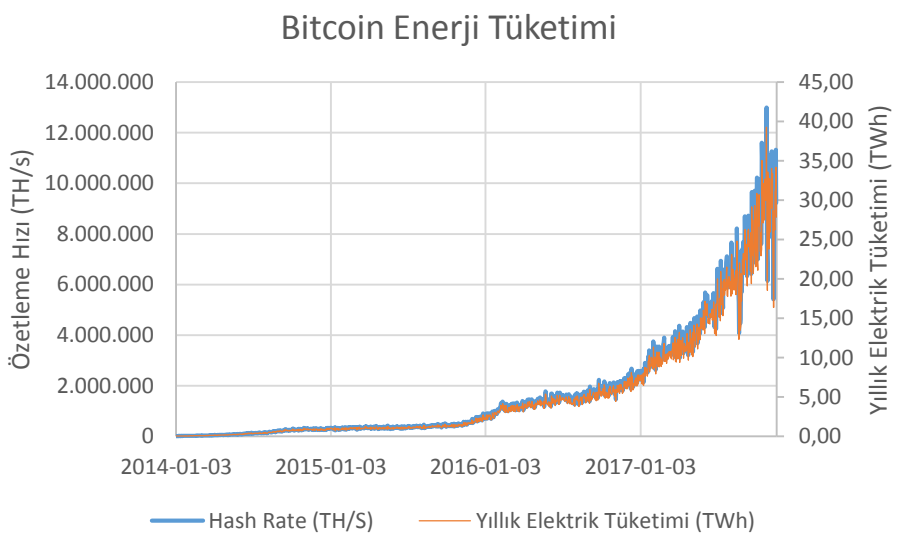
7- Açık Kayıt Zinciri Ekonomik Modeli

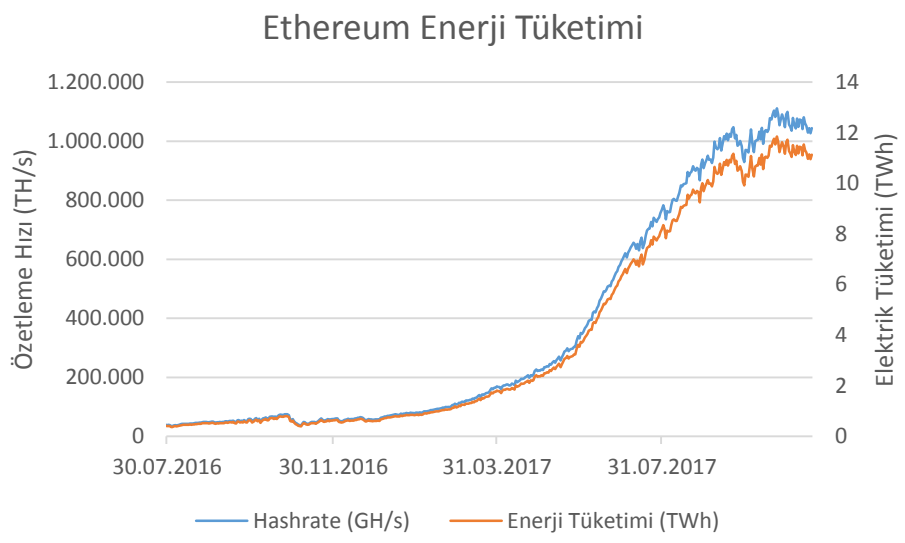
$$P_{net} = \frac{R_{net}}{\varepsilon}$$

R_{net} → Özetleme Hızı (Hash Rate)

ε → İşlemcinin Enerji Verimliliği

Mutabakat Mekanizmaları
Kriptografik Teknoloji
İşlemci Teknolojileri





Yerli Silikon Vadisi Yatırımları Desteleme Mekanizması?
Yeni Elektrik Fiyatlama Mekanizmaları?

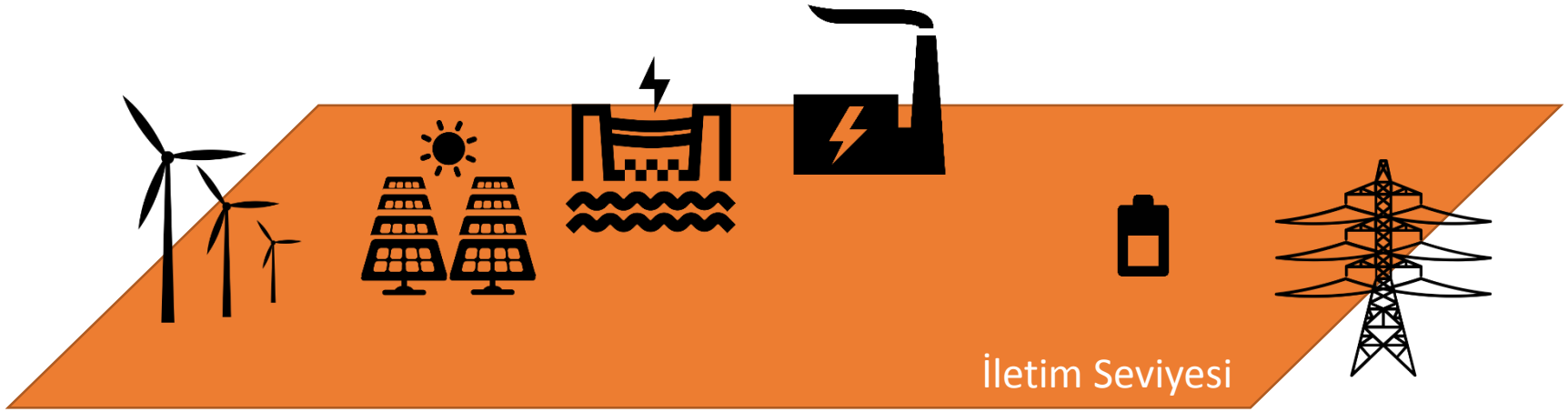
WORLD ENERGY COUNCIL TURKEY TÜRK MİLLİ KOMİTESİ

http://eprints.maynoothuniversity.ie/6009/1/DM-Bitcoin.pdf

8- Elektrik Sektöründe Değişim

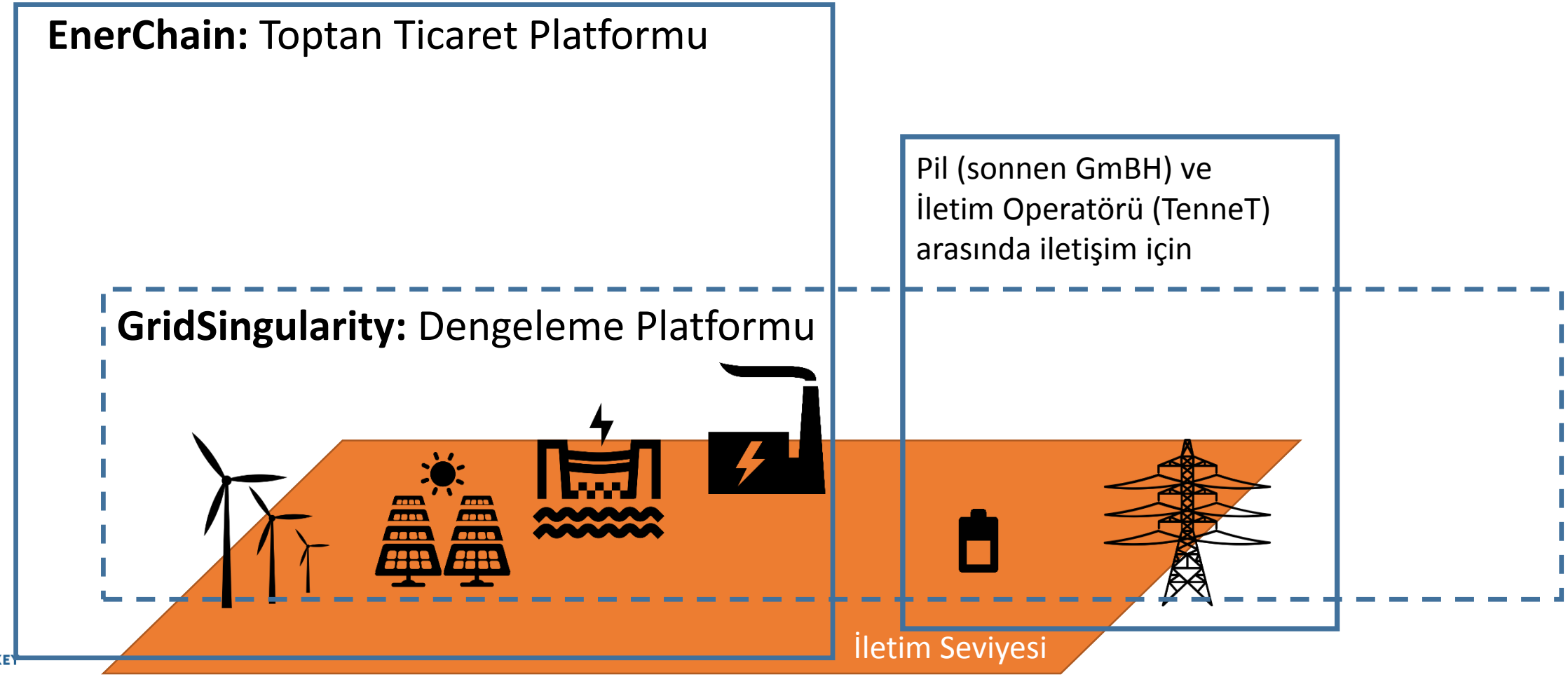
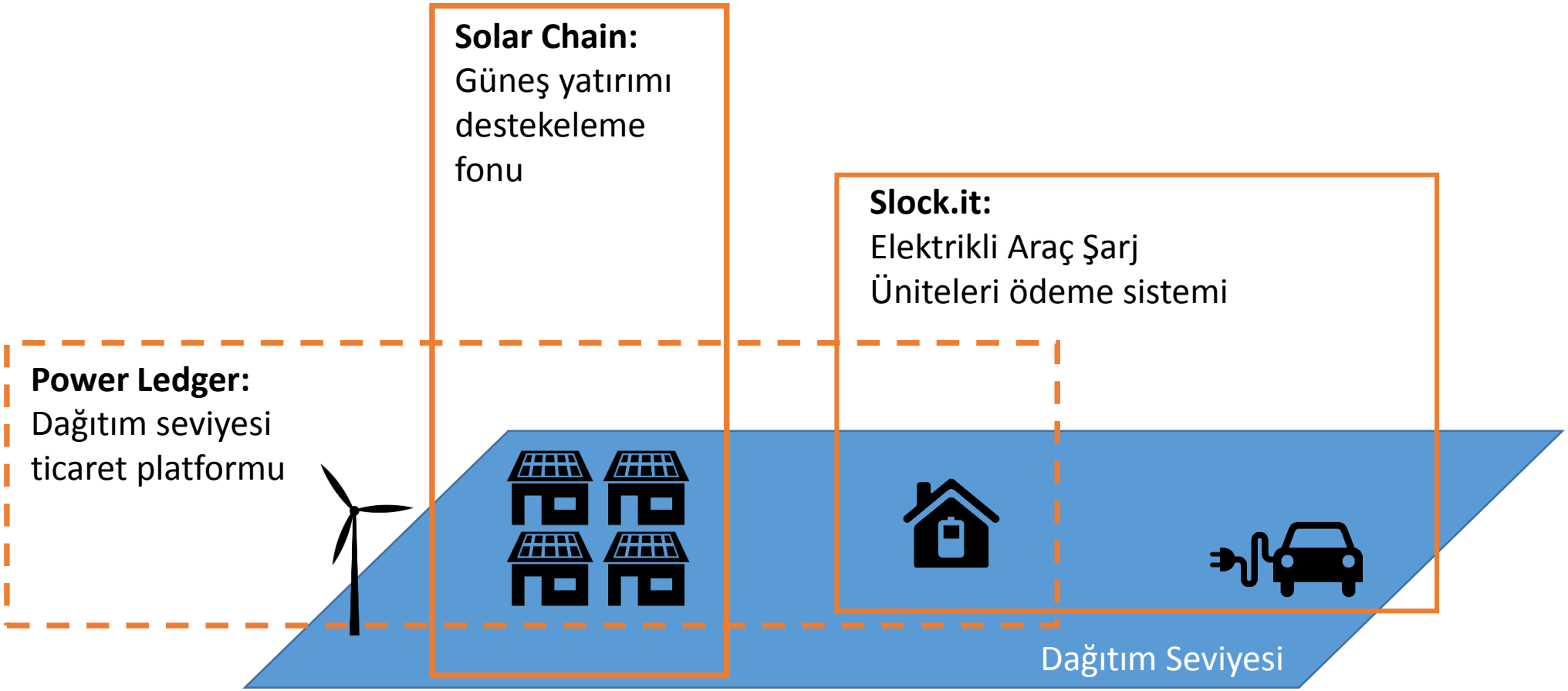
Fosil Yakıtlı Üretim	İletim	Dağıtım	Perakende & Serbest Tüketici	Üreten Tüketici
- Elektrik üreticisi - Piyasa bazlı karlılık	- Üreticiden dağıtıma	- İletimden müşteriye	- Fosil Üreticiden müşteriye satış	- Göz ardı edilen üretim - Sisteme elektrik üretim fazlasını satar
- Esneklik sağlayıcı - Yan hizmetler karlılık	- Esnekliğin başlangıcı - Yenilenebilir yönetimi	- Yenilenebilir yönetimi - Dağıtık sistem akışı	- Hizmet sağlayıcı - Danışmanlık - Finansal Kiralama	- Popüler - Dağıtım dengeleme - Pilin gücü

9- Enerji ve Kayıt Zinciri



WORLD ENERGY COUNCIL | TURKEY TÜRK MİLLİ KOMİTESİ

9.1- Kapalı Zincir Uygulamaları



9.2- Açık Zincir Uygulamaları