

1.Bölüm

- Finans nedir?
- Teknoloji nedir?
- Finans ve Teknolojinin birlikteliği: Fintech
- Fintech ve Geleneksel Finansal Hizmetler Arasındaki Farklar
- Fintech'lerin Kullanıcılarının Hayatlarına Kattığı Değerler
- Dünya'da ve Türkiye'de Fintech örnekleri

Dersin Sorumlusu: Öğr. Gör. Olcay YILMAZ

1. Hafta Kaynakları: Ahmet Usta, Serkan Doğanterkin, 2018. Blockchain 101.

Chris Skinner, 2015. Waluweb.

İyzico, 2019. Fintech Nedir? Finans sektöründeki etkileri nelerdir?

İTÜ Çekirdek, 2018. Dünyü, bugünü, yarını: 5 maddede fintech nedir?

GBA, 2018. Girişimciler için Fintech akımına ilk bakış

Para durumu, 2018. Fintech alanında girişimciliğin Türkiye'deki geleceği

Finans Nedir?

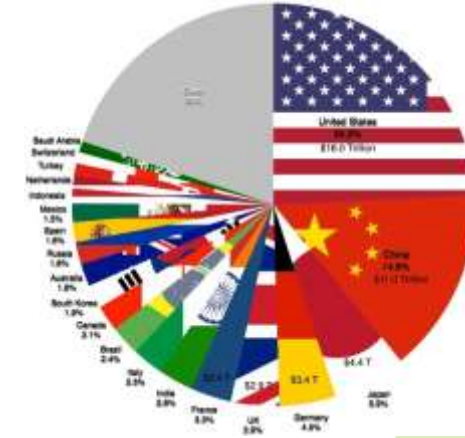
Etimolojik olarak «Para, sermaye» olarak tanımlanan, dilimize Fransızcadan giren Finans kelimesi; ihtiyaç duyulan fonların «uygun şartlarda» sağlanması, etkin bir şekilde kullanılması ile ilgili faaliyetlerin bütünü olup, bilim dalı olarak işletme ve ekonomi disiplinlerinin ortak dalıdır.



Bireysel
Finans



Kurumsal
Finans



Kamusal
Finans

Teknoloji nedir?

- Günlük yaşantımızda gerçekleştirdiğimiz eylemlerin süresini kısaltan;
- Bu eylemlerin kalitesini artıran;
- Hayatımızda daha önce var olmayan ürün ve hizmeti yaşantımıza dahil eden yeniliklerdir.





Kaynak: <https://www.telecommute.org/the-uses-of-technology-in-our-life/>



Kaynak: <https://www.pdsol.com/news/what-is-industry-4-0/>

Paranın evrimi



Takas



Altın



Metal paralar



Kağıt paralar



Plastik kartlar



Elektronik para



Kripto para birimi

Kaynak: <https://twitter.com/btcanaliz/status/1089608789299478529/photo/1>

Finans ve Teknolojinin Birlikteliđi: Fintech

- Finans ve teknoloji kelimelerinin birleşmesiyle meydana gelen ve «financial Technologies» kısaltması olarak literatürde yer edinen «fintech», teknolojinin finans sektörüne dokunmasıyla geleneksel yolla sunulan finansal ürün ve hizmetlerin daha etkin, hızlı, kolay, güvenilir sunulmasını ilke edinmiş bir konsept, inovasyon, endüstridir.
- Fintech girişimleri, müşterilerinin hayatlarını kolaylaştırma felsefesiyle hareket etmektedir.
- Özetle; teknolojinin paraya dokunduđu her örnek, fintech başlığına konudur.

Fintech'in ortaya çıkış serüveni



Fintech ve Geleneksel Finansal Hizmetler Arasındaki Farklar



Mobile endeksli uygulamalar vasıtasıyla tüm geleneksel finans hizmetlerini cebe sığdırmak



Banka hesabı açmak, fatura ödemek, sigorta yaptırmak, kredi çekmek, eft-havale-swift yapmak için birçok evrakla banka şubesine gitmek

Fintech'lerin Kullanıcılarının Hayatlarına Kattığı Değerler

Pratiklik,
Zaman
tasarrufu

Fiyat Avantajı

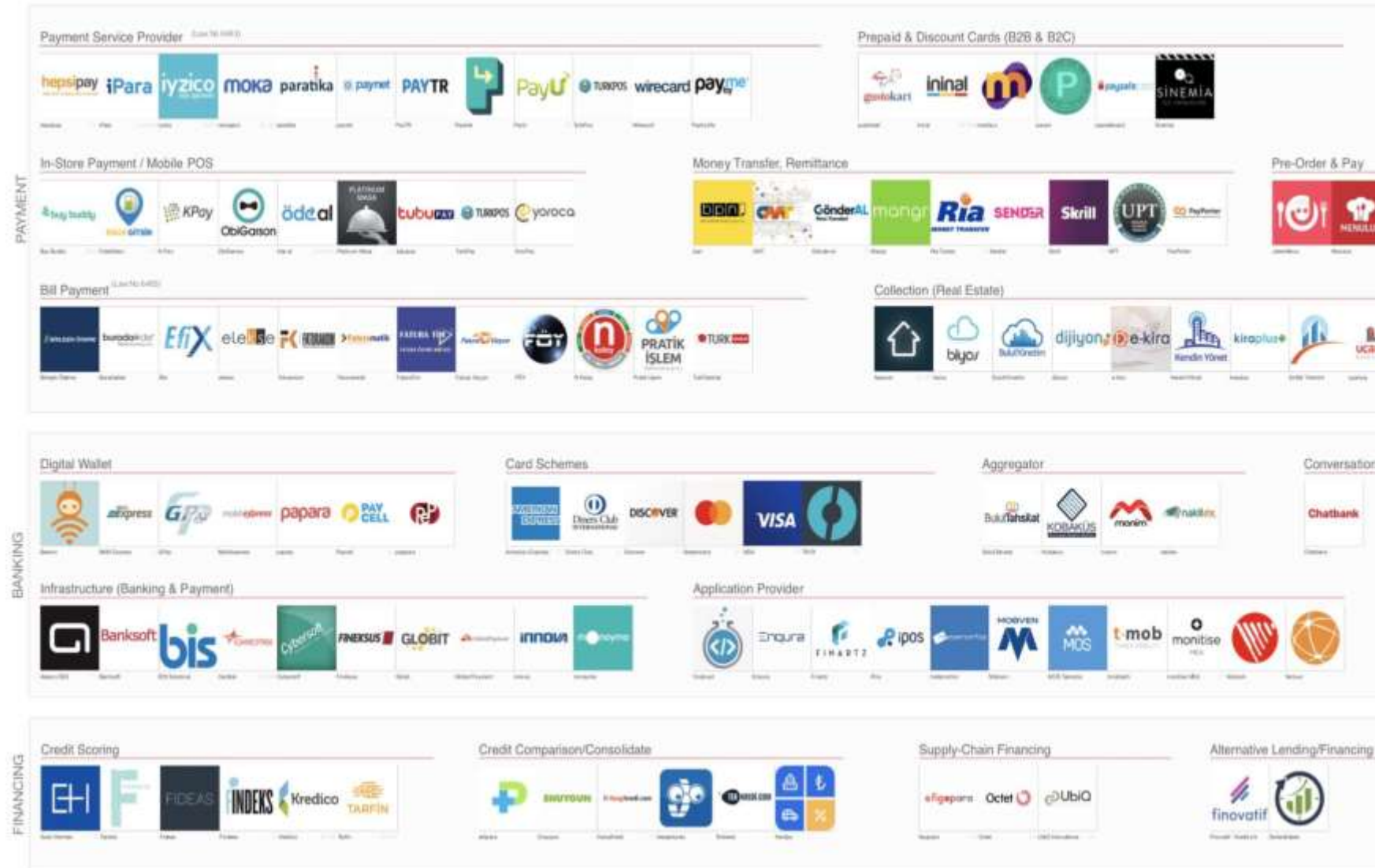
Daha Fazla
Hizmet
Seçeneđi

Kişiselleştirilmiş
Deneyim

Türkiye’de Fintech örnekleri



Türkiye’de Fintech örnekleri



Türkiye'nin En değerli Fintech Şirketleri



Colendi: 700 milyon dolar değerlemeye ulaşan Colendi, yapay zeka destekli uçtan uca finansal çözümler sunuyor. Kullanıcılarının finansal hizmet altyapılarını geliştirerek bu alanda küresel pazarda büyümeyi hedefliyor.



Papara: Türkiye'nin en tanınan dijital cüzdan ve ödeme uygulamalarından biri olan Papara, kullanıcılarına anlık ödeme, para transferi ve çeşitli finansal hizmetler sunuyor. Özellikle genç kitleler arasında yaygın olarak kullanılıyor.

Türkiye'nin En değerli Fintech Şirketleri



Iyzico: Özellikle e-ticaret sitelerine yönelik ödeme altyapıları sunan Iyzico, güvenli ve hızlı ödeme çözümleri sağlıyor. Avrupa'ya açılarak küresel pazarlarda da etkinlik gösteriyor.



Finekra: İşletmelerin finansal süreçlerini yönetmelerine yardımcı olan Finekra, online tahsilat ve POS raporlama gibi çözümler sunuyor ve değerlemesi 20 milyon doları aşmış durumda.

Dünya'da Unicorn olmuş Fintech Girişimleri

The Stripe logo is displayed in a bold, blue, sans-serif font.

Stripe (ABD)

Hizmetler: Çevrimiçi ödeme altyapısı ve finansal araçlar sunar. Büyük şirketlere (Amazon, Meta, Microsoft) hizmet verir.

Değer: Yaklaşık 50 milyar dolar.



Revolut (Birleşik Krallık)

Hizmetler: Neobank olarak geniş kapsamlı bankacılık hizmetleri, uluslararası para transferleri, kripto para yatırımları.

Değer: 33 milyar dolar.

Dünya’da Unicorn olmuş Fintech Girişimleri



Nubank (Brezilya)

Hizmetler: Dijital bankacılık, kredi kartları ve sigorta hizmetleri. Latin Amerika'nın en büyük fintech firması.

Değer: 41.5 milyar dolar.



Klarna (İsveç)

Hizmetler: "Buy Now, Pay Later" modeliyle post-purchase ödeme çözümleri.

Değer: 46 milyar dolar.

Dünya’da Unicorn olmuş Fintech Girişimleri



Robinhood (ABD)

Hizmetler: Komisjonsuz hisse senedi ve kripto para ticareti.

Değer: 9 milyar dolar.



Adyen (Hollanda)

Hizmetler: Ödeme altyapısı sağlayıcısı, global ödeme hizmetleri sunar.

Değer: 17 milyar dolar.

2.Bölüm

- ▶ Nedir bu Bitcoin? Bitcoin Hakkında Bilinmesi Gereken Temel Konular
- ▶ Bitcoin önderliğinde Kriptoparalar ve Blokzincir altyapılarının Temel Özellikleri
- ▶ Bitcoin Hakkında İtiraz ve Eleştiriler
- ▶ Bitcoin Mevcut Düzene karşı (Anarko yapısı)
- ▶ Bitcoin Balon mu?
- ▶ Bitcoin Saadet Zinciri mi?
- ▶ Bitcoin'in İçsel Değeri
- ▶ Bitcoin Para mıdır?
- ▶ Bitcoin'in Temel Sıkıntıları

Dersin Sorumlusu: Öğr. Gör. Olcay YILMAZ

Kaynak: Vedat Güven, Erkin Şahinöz. Blokzincir, Kripto Paralar, Bitcoin, 2018.

Nedir Sahi bu Bitcoin?



Kaynak: <https://www.openaccessgovernment.org/what-is-bitcoin-cryptocurrency/42401/>

Sanal para? Dijital para? E-para? Kripto Para?



Kaynak: <https://wiredworksjax.com/faq/>

Kripto derken?



Kaynak: <https://www.ziraatbank.com.tr/tr/dijital-bankacilik/mobil-bankacilik/ziraat-mobil>

Kriptodan kasıt, internet/mobil bankacılığa girerken kullandığımız şifre değildir. Karşılığı parasal değer olan bilgisayar kaydının (verinin, işlemin) şifrelenmiş halidir BİTCOİN.

Kriptoloji: Şifre Bilimi.

Kriptografi: Verilerin, yazıların şifrelenmesi.

Ödeme yapmanın «En hızlı ve güvenilir» yolu nedir?



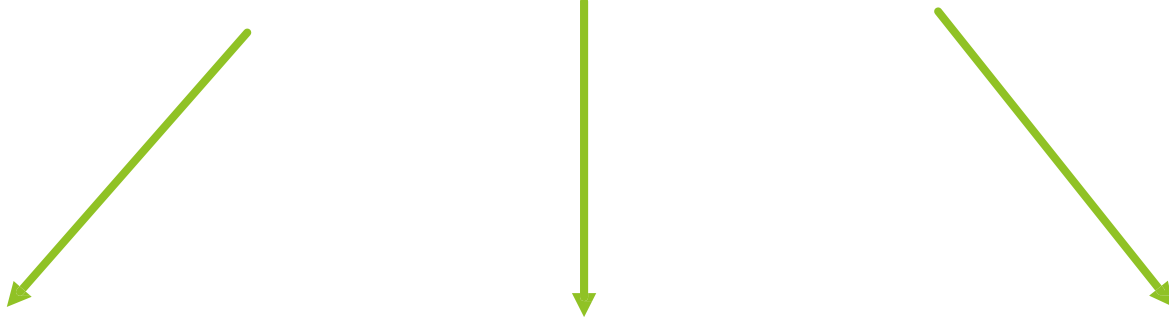
Kaynak: <https://abcnews.go.com/Health/bacteria-live-money/story?id=23413718>

Gerçek hayatta «pratik ve güvenilir»
olsun diye hep yüz yüze mi olacağız?

*21.y.y. Önem arz eden konularının
başında gelmektedir ödemeyi,
transferi yanında olmadığımız
kişi/kuruma pratik bir şekilde yapmak...*



- ▶ En sade ifadeyle; bir aracı olmadan, (p2p) eşten eşe güvenilir bir şekilde para transferi ve ödeme yapmayı mümkün kılan geleceğin para birimi ADAYIDIR.
- ▶ Yüz yüze yapılan işlemi yüz yüze değilken de yapabilmektedir.
- ▶ Hocam, EFT? HAVALE? SWIFT?



Hepsinde aracı kurum var.

Komisyon var. Datalarınız, bilgileriniz, mahremiyetiniz aracı kurum ile paylaşılıyor.

Swift işleminde yüksek komisyona ilaveten zaman maliyeti de var.



•Cep telefonunuzdaki uygulamayı (Mobil cüzdanlar) kullanarak Dünya'nın istediğiniz yerindeki kişiye, kuruma, istediğiniz zamanda (hafta sonu, gece yarısı) ödeme yapabilme, para transferi gerçekleştirebilmektesiniz.

•Sistemin kuralları öyle güvenli kurgulanmış ki (matematik, yazılım, algoritma) kimse olmayan parasını bir başka adrese 2. defa transfer edemediği gibi, daha önce harcanan para 2. defa harcanamıyor.

Eşten eşe (P2P), çok düşük ücretli (Son dönemlerde komisyonlar yükseliyor), Dakikalar içerisinde (Son dönemlerde bekleme süreleri uzuyor) 3. partilere (Aracı kurumlar) ihtiyaç duymaksızın ödeme ve transfer yapılabiliyor.

*Bitcoin'in 2009 yılında ortaya çıkış felsefelerindendir; aracısız, maliyetsiz, anlık değer transferi. Yukarıdaki parantez içerisindeki komisyonların artması ve işlem sürelerinin uzamasının sebepleri olarak, artan işlem hacmi ile **madencilerin?!** gelir elde etmek istemeleri gösterilebilir.*

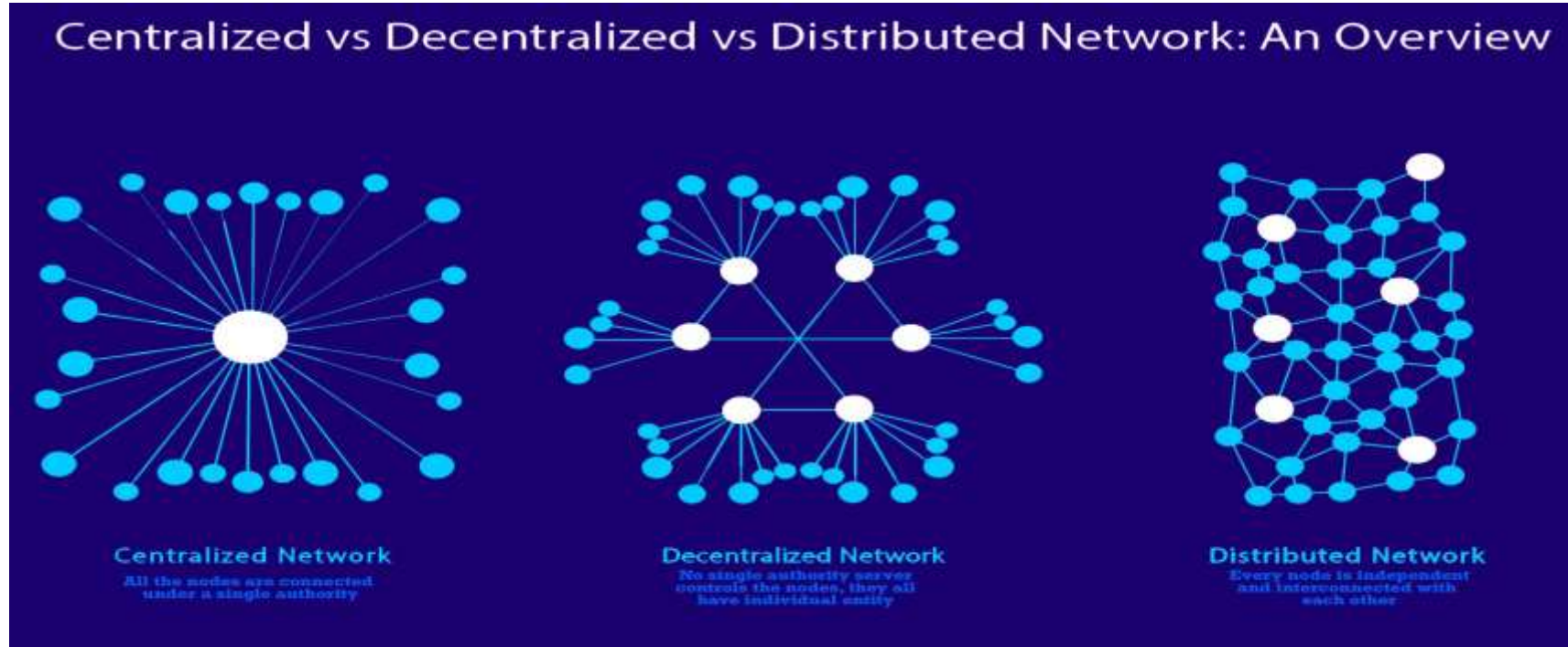
Madenciler derken?



- *Sistemin çalışması, gerçekleşecek işlemlerin kaydı, doğrulanması ve kripto paraların keşfedilmelerini sağlayan bilgisayar ağına katılan kişilerdir. Özetle, blokzincir teknolojisinin bloklarını oluşturan emekçilerdir.*

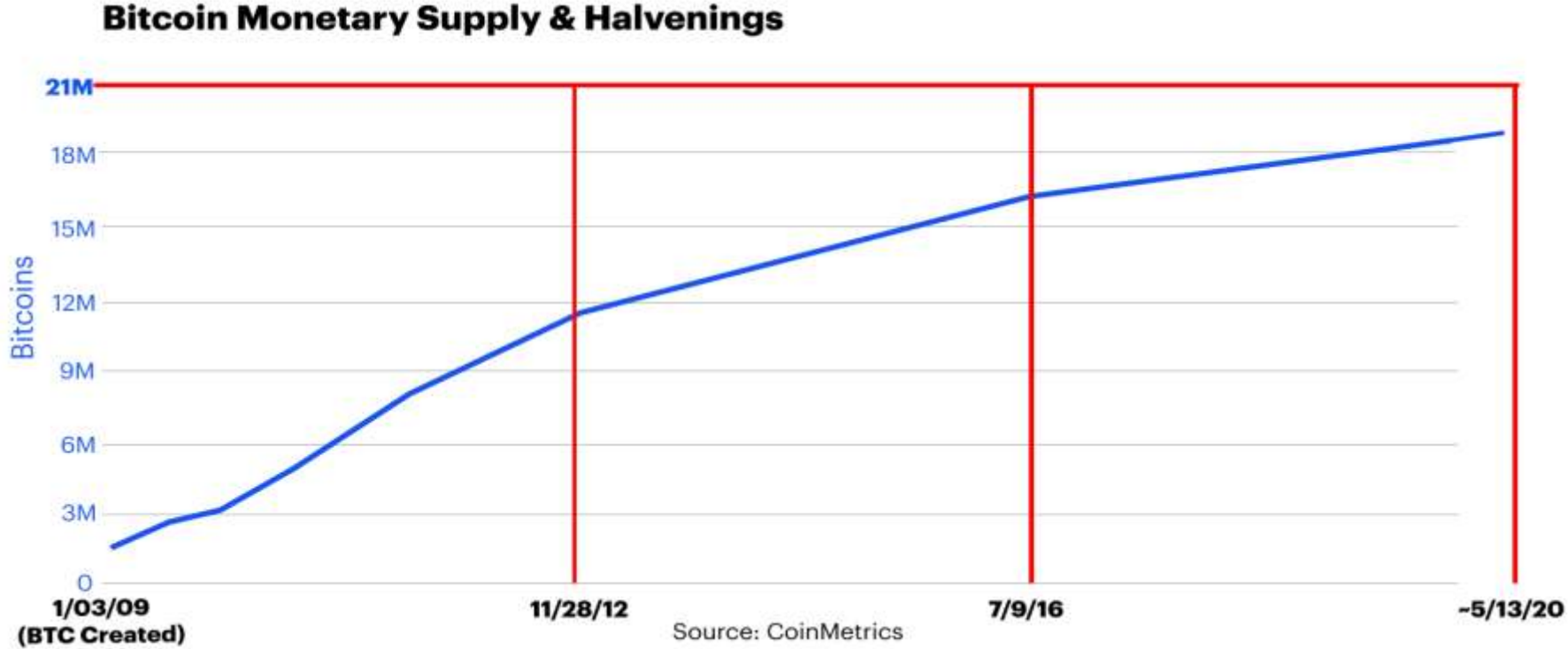
Bitcoin önderliğinde Kripto paralar ve Blokzincir altyapılarının Temel Özellikleri

- Merkeziyetsiz (Adem-i Merkezi) olmaları - Arkada herhangi bir Devlet yahut Merkez Bankası yok.
- Dağıtık bir mimariye sahip olmaları (*Hacklenme/siber saldırı esnasında merkezi bir sunucu yok*)



Arza konu olacak para miktarının baştan belli olması (Bkz: 21 Milyon adet Bitcoin - Böylece Devletlerin para basarak kendilerine gelir yaratmasının, enflasyon ile halkın omuzlarına yük binmesinin söz konusu olmaması)

Kuralları Baştan Çizilmiş Bitcoin'in Yıllara Göre Arz Miktarı: Toplam 21 milyon Adet



Kaynak: <https://blog.coinbase.com/digital-gold-scarcity-and-bitcoin-halvings-1d6cc16f3e8d>

Bitcoin Hakkında İtiraz ve Eleştiriler

İşlem takibinin mümkün olmaması

Blockchain.com

Cüzdan

Takas

Explorer

Bitcoin Satın Al

Ticaret

Son Bloklar

Yükseklik	Mayınlı	Madenci	Boyut
652395	15 dakika	AntPool	1.397.747 bytes
652394	34 dakika	F2Pool	1.249.418 bytes
652393	41 dakika	AntPool	1.365.378 bytes
652392	45 dakika	SlushPool	1.368.440 bytes
652391	53 dakika	SlushPool	1.371.222 bytes
652390	1 saat	Unknown	1.418.047 bytes

Tüm Blokları Görüntüle →

Son İşlemler

Hash	Zaman	Miktar (BTC)	Tutar (USD)
0fe2789a2be8bd085fe48...	17:24	0.01472339 BTC	\$169,18
bb909304b55162c5d1b6...	17:24	0.01069246 BTC	\$122,87
7cf808a41ef35f89e87378...	17:24	8.66013074 BTC	\$99.512,61
17efbbd730928fa37af866...	17:24	1.96164429 BTC	\$22.541,04
3a277564458dbdd8629...	17:24	0.11445370 BTC	\$1.315,17
02f69be2acaa0bf622728...	17:24	0.01808476 BTC	\$207,81

Tüm İşlemleri Görüntüle →

Kaynak: https://www.blockchain.com/tr/explorer?utm_campaign=expnav_explorer

Yeraltı ekonomisi (kayıtdışılık, kaçakçılık, kara para aklamadaki payı)



Bitcoin Mevcut Düzene karşı (Anarko yapısı)

- *Bitcoin'e gösterilen esas itiraz ve direncin kaynağıdır Anarko yapısı.*

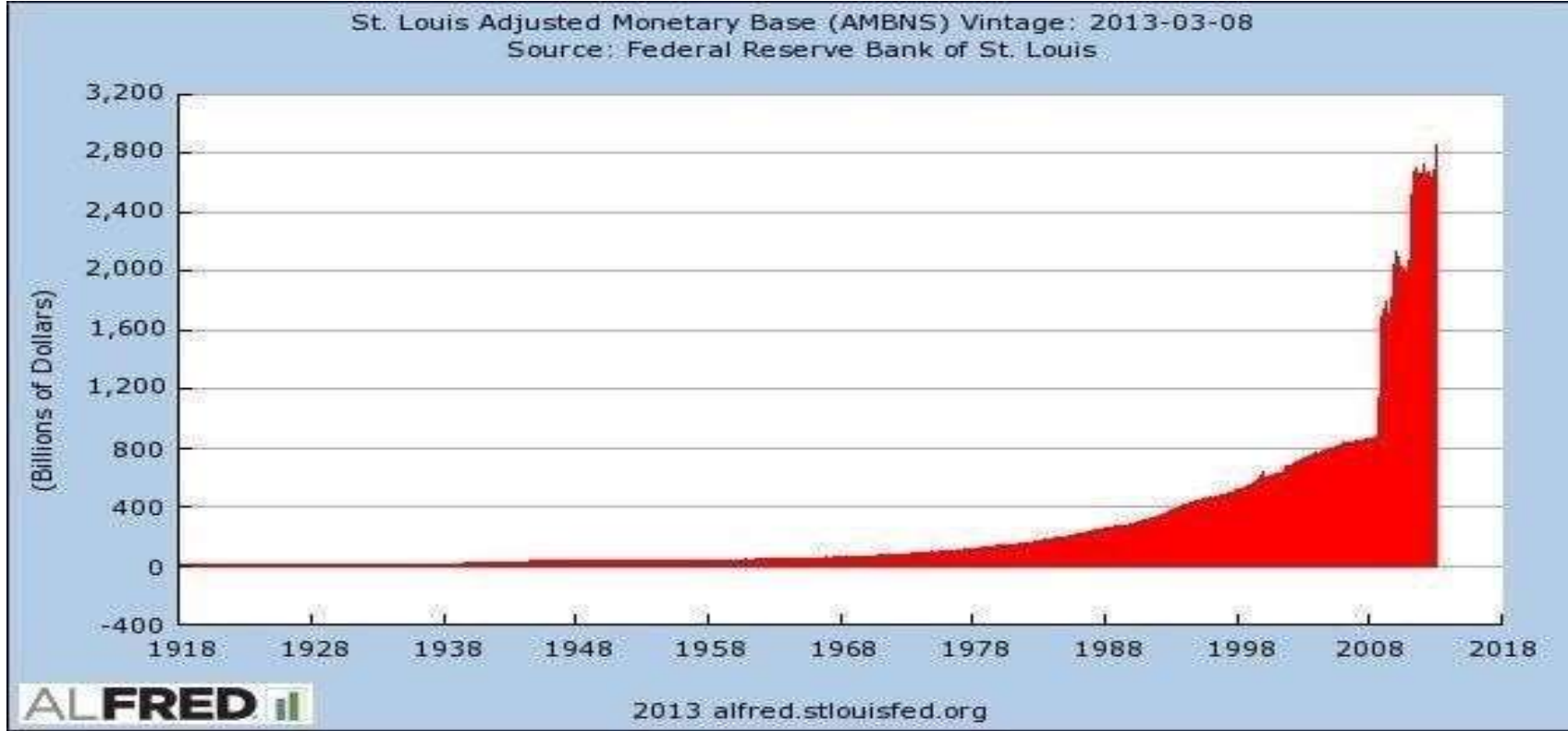
- *Merkeze bağlı değil.*
 - *Devlet tarafından ihraç edilmiyor.*
 - *Bilgi ve veriler Devlet elinde depolanmıyor.*
- *Devletlerin senyoraj gelirleri ellerinden alınıyor.*
 - *Bir kişinin değil, herkesin parası.*

Zimbabwe’de Hiperenflasyon ve Halkın Bitcoin Kullanımının Yaygınlaşması (2017)



Kaynak: <https://businesstimes.co.zw/zim-will-not-plunge-into-hyper-inflation-again-rbz/>
<https://www.csmonitor.com/World/Africa/2008/0325/p06s02-woaf.html>

2008 Küresel Ekonomik Krizi Sonrası ABD merkez Bankası FED'in Trilyonlarca \$ Karşılıksız Para Basması



Kaynak: https://www.reddit.com/r/Bitcoin/comments/7guh08/this_bitcoin_chart_is_insane_oh_wait_thats/

2013 Yunanistan Ekonomik Krizi ve Halkın Kendi Parasını ATM'lerden Limitli Çekebilmesi



Kaynak: <https://www.dw.com/en/capital-controls-greece-can-learn-from-cyprus/a-18550302>

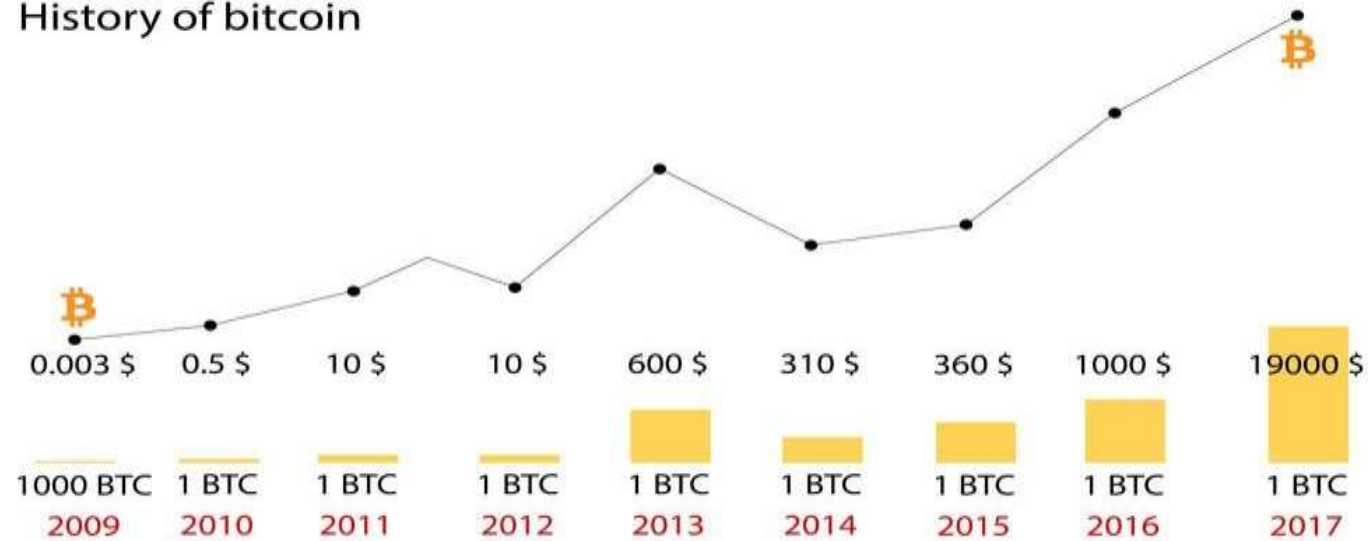
Savaş, Çatışma, Soykırım sebebiyle Yurtlarını Terkeden Mülteci, sığınmacı, göçmenler için Bir Çözüm: BTC



Kaynak: <https://turksam.org/turksam-goc-gocmen-bulteni-23-mayis-2018>
<https://turksam.org/turksam-goc-gocmen-bulteni-7-mayis-2018>
https://insamer.com/tr/avrupada-kayip-refakatsiz-multeci-cocuklar_2331.html

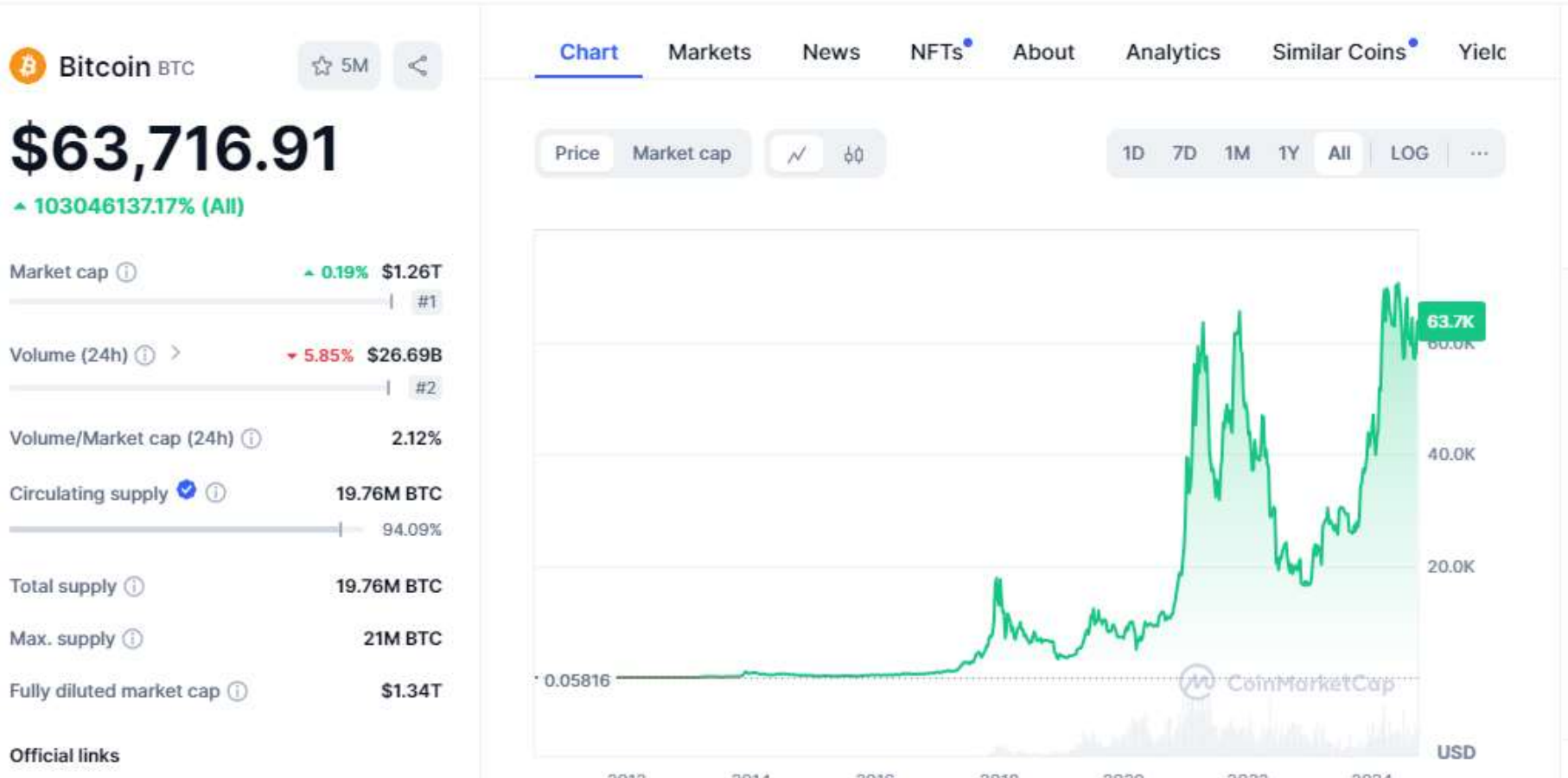
Bitcoin Balon mu?

History of bitcoin



Kaynak: <https://www.vectorstock.com/royalty-free-vector/bitcoin-price-history-infographics-of-changes-vector-19654594>

Bitcoin Balon mu?

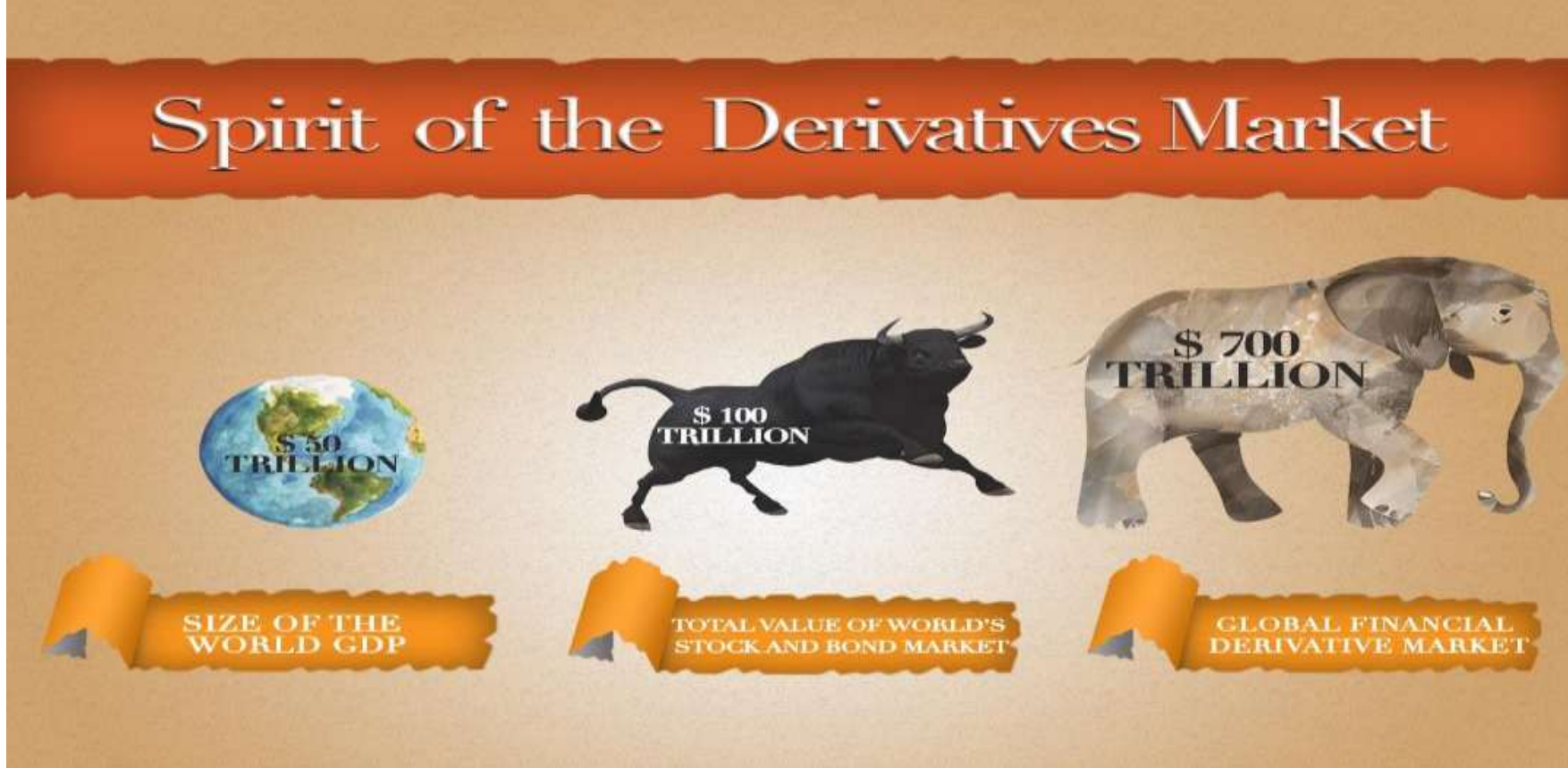


Kaynak: <https://coinmarketcap.com/currencies/bitcoin/> (24.09.2024)

Kripto Paraların Piyasa Değeri

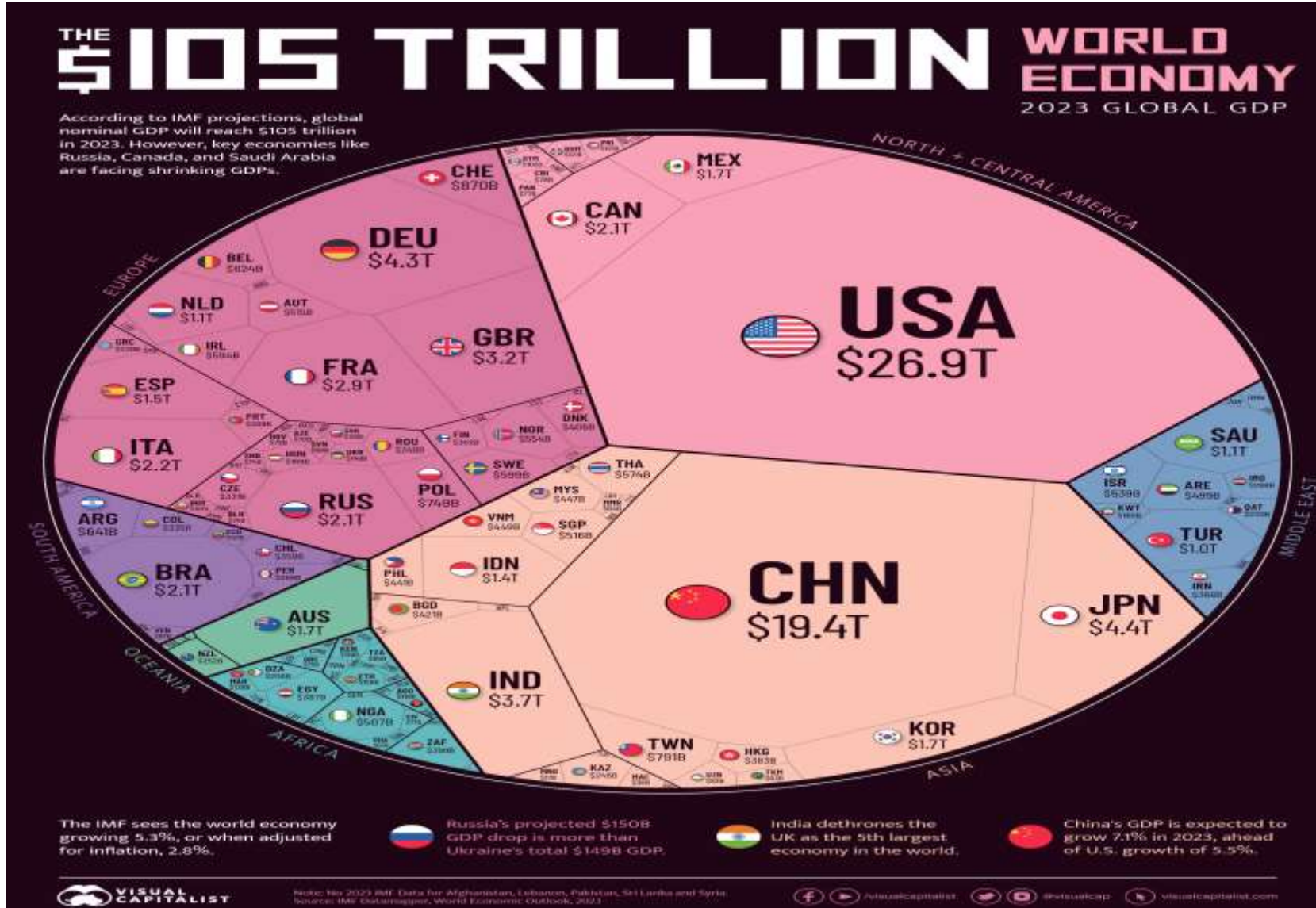
Cryptos: 2.4M+ Exchanges: 795 Market Cap: \$2.24T ▲0.69% 24h Vol: \$68.39B ▼2.70% Dominance: BTC: 56.3% ETH: 14.3%									
#	Name	Price	1h %	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ	Last
☆ 1	Bitcoin BTC	\$63,786.91	▲0.51%	▲0.49%	▲8.57%	\$1,260,317,506,187	\$26,718,524,426 419,367 BTC	19,758,246 BTC	
☆ 2	Ethereum ETH	\$2,663.82	▲0.84%	▲0.89%	▲15.28%	\$320,622,722,237	\$16,569,387,632 6,241,269 ETH	120,362,208 ETH	
☆ 3	Tether USDT	\$1.00	▼0.00%	▲0.01%	▲0.02%	\$119,253,521,957	\$52,179,236,512 52,183,688,219 USDT	119,243,573,831 USDT	
☆ 4	BNB BNB	\$605.08	▲0.50%	▲2.61%	▲12.35%	\$88,301,403,683	\$2,125,930,561 3,519,229 BNB	145,933,430 BNB	
☆ 5	Solana SOL	\$148.05	▲1.05%	▲2.97%	▲11.65%	\$69,394,046,508	\$2,289,423,969 15,489,165 SOL	468,730,922 SOL	
☆ 6	USDC USDC	\$1.00	▼0.00%	▲0.02%	▲0.01%	\$35,908,482,808	\$5,319,441,023 5,319,700,395 USDC	35,900,495,864 USDC	
☆ 7	XRP XRP	\$0.5877	▲0.17%	▲0.09%	▲0.55%	\$33,168,754,616	\$898,196,027 1,529,205,019 XRP	56,434,507,880 XRP	

Türev Piyasalar Deęeri



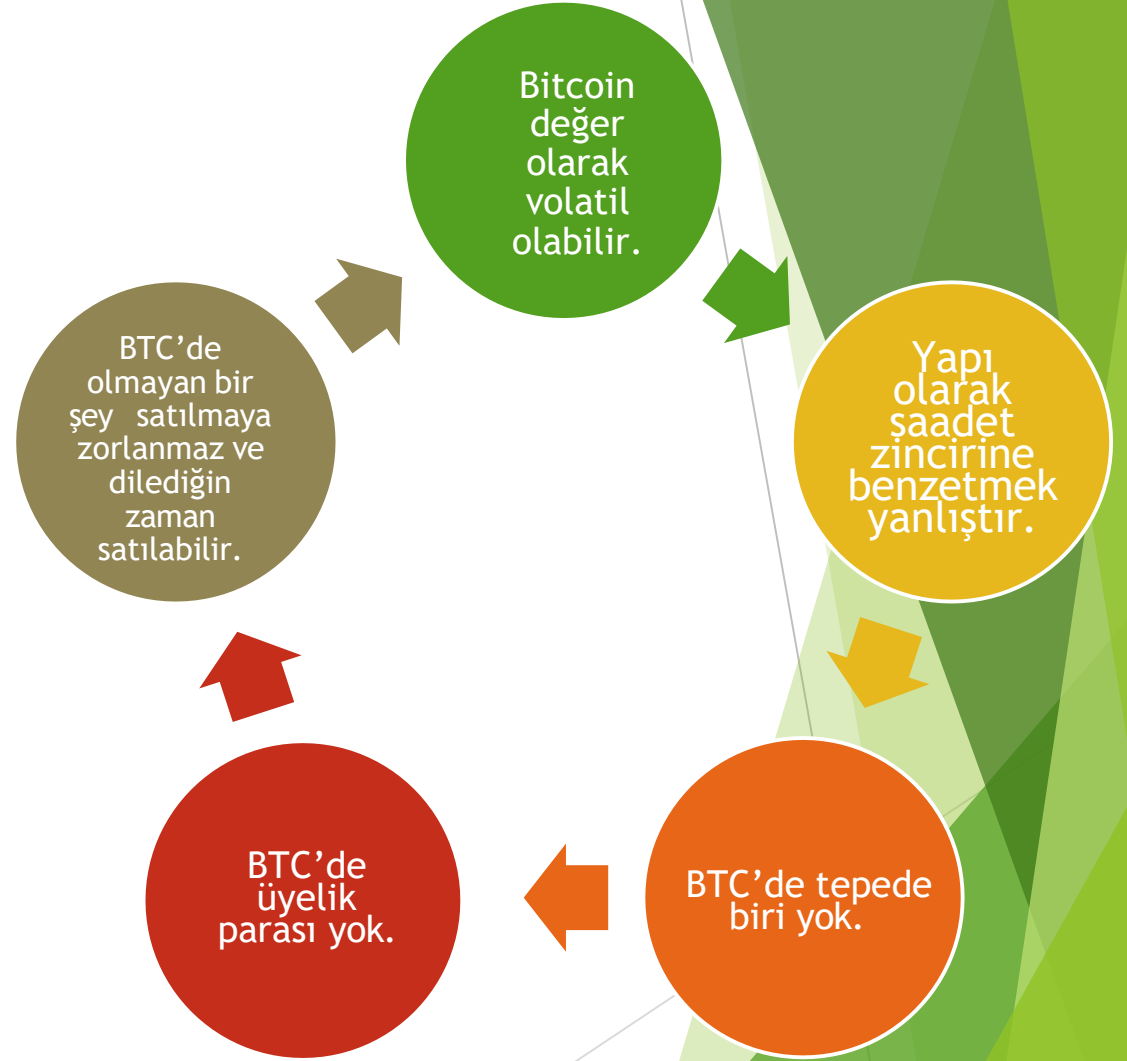
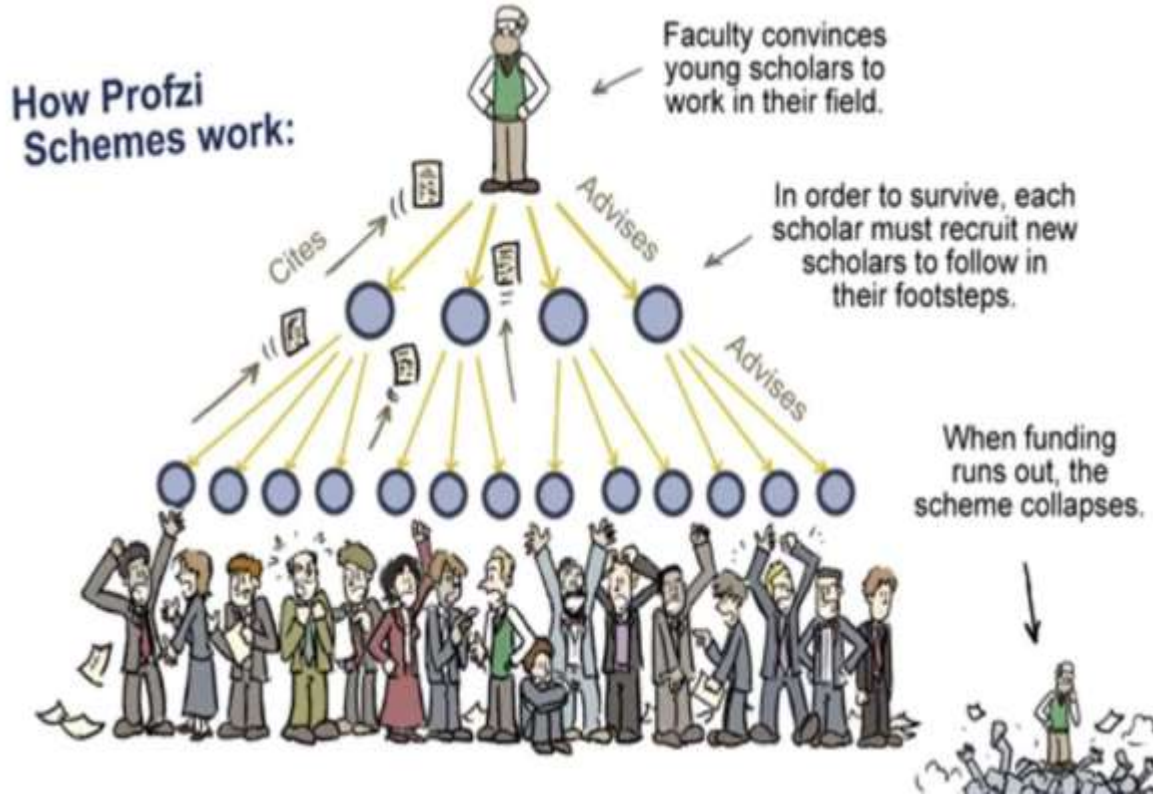
Kaynak: <https://www.mudraksh.com/2017/10/27/derivative-traders-confessions/>

Dünya GSYİH değeri = 105 Trilyon \$ (2023)



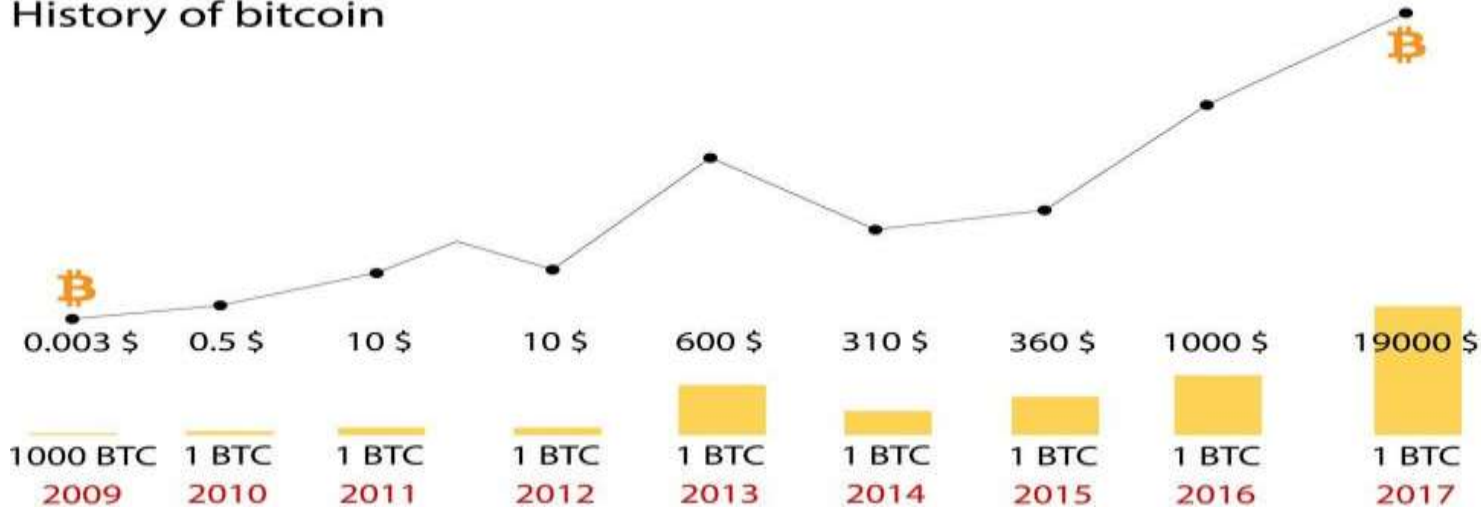
Bitcoin Saadet Zinciri mi?

Saadet zinciri derken?



Bitcoin'in İçsel Değeri (Olması gereken Reel değer)

History of bitcoin



Soruya soru: Dolar'ın, TL'nin içsel değeri nedir?

2024 yılı ABD altın rezervi
8130 ton = 630 milyar \$
ABD'de 21 trilyon dolar
yaklaşık 30 kat
büyüklüğünde
karşılıksız basılmış para
var.

2024 yılında TR'de 550 ton
altın stoku var, yaklaşık 1,6
trilyon TL yapar tedavülde
ise 15 trilyon TL.
(Yaklaşık 10 katı)

Not: Karşılıksız para basan devlet
itibarına güveniyor (Askeri,
ekonomik, teknolojik, kültürel
gücüne)

► Değer kavramları baştan yazılırken...



69 milyar \$ piyasa değeri



26 milyar \$ piyasa değeri

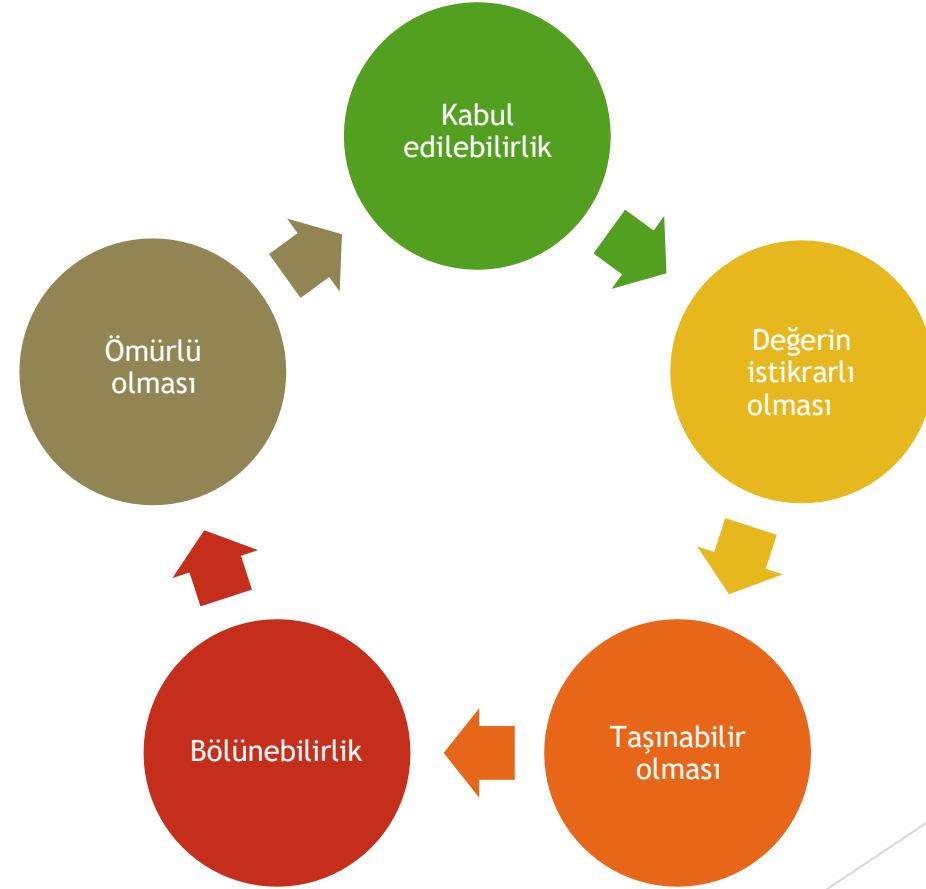
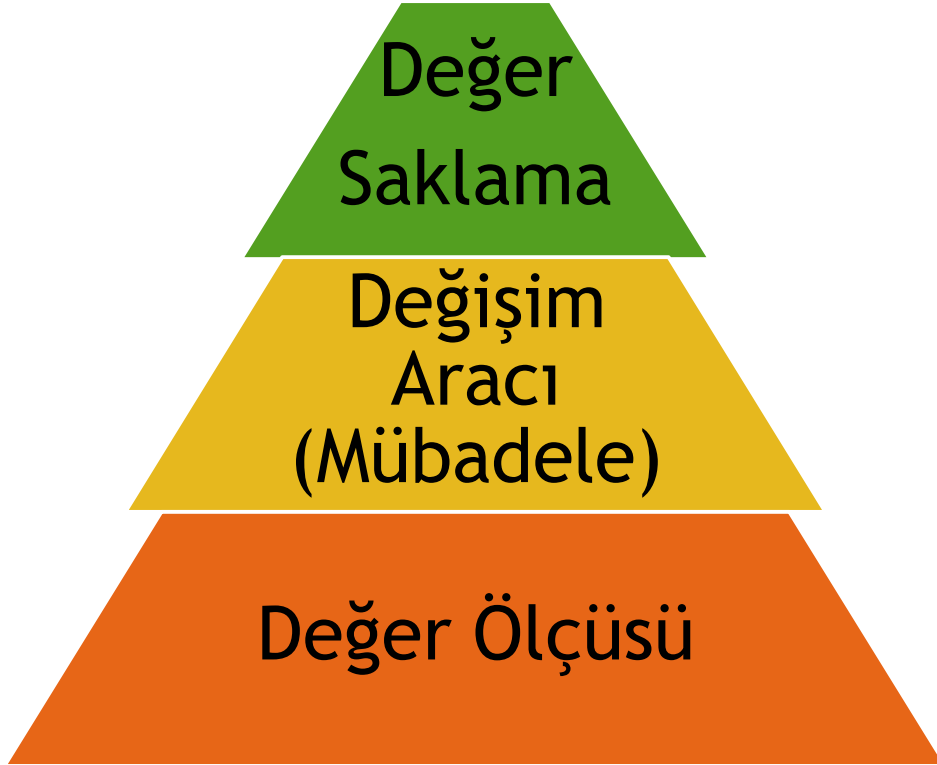


- **Arkada yatan teknoloji**
- **Güven,**
- **Matematik,**
- **Yazılım,**
- **Toplumun kendisine atfettiği değer**

Bitcoin Para mıdır?

Paranın Klasik Fonksiyonları

Paranın Geniş Özellikleri



Bitcoin'in Temel Sıkıntıları



İşlemlerin düzenli sürmesi için oluşturulan bloklar için harcanan yüksek enerji miktarı

Volatilite



Gelenekselde var olan sıkıntılar

- *Banknotların basımı, dağıtımı, eskiyen ve yıprananların ortadan kaldırılması;*
- *Banknotların sahtelerinin üretilmemesi, kalpazanların takibi ve yakalanması için harcanan işgücü ve enerji;*
- *Bankacılık sisteminin hacklenmemesi için harcanan milyar \$'lar*

İleri dönemlerde yenilenebilir enerji ile (güneş, rüzgar, biyogaz vs.. Maliyetlerin minimizasyonu öngörülmektedir.

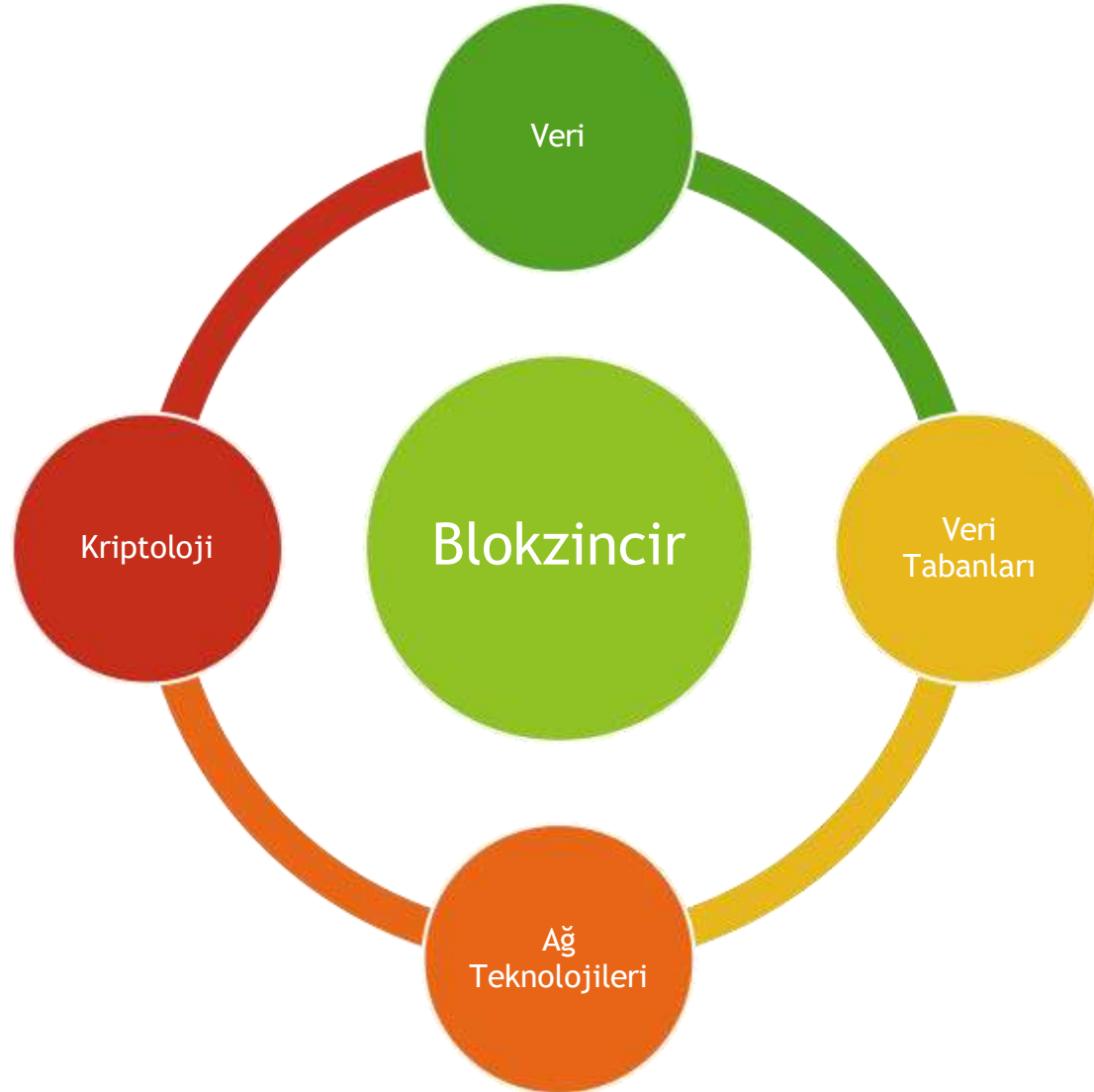
3.Bölüm

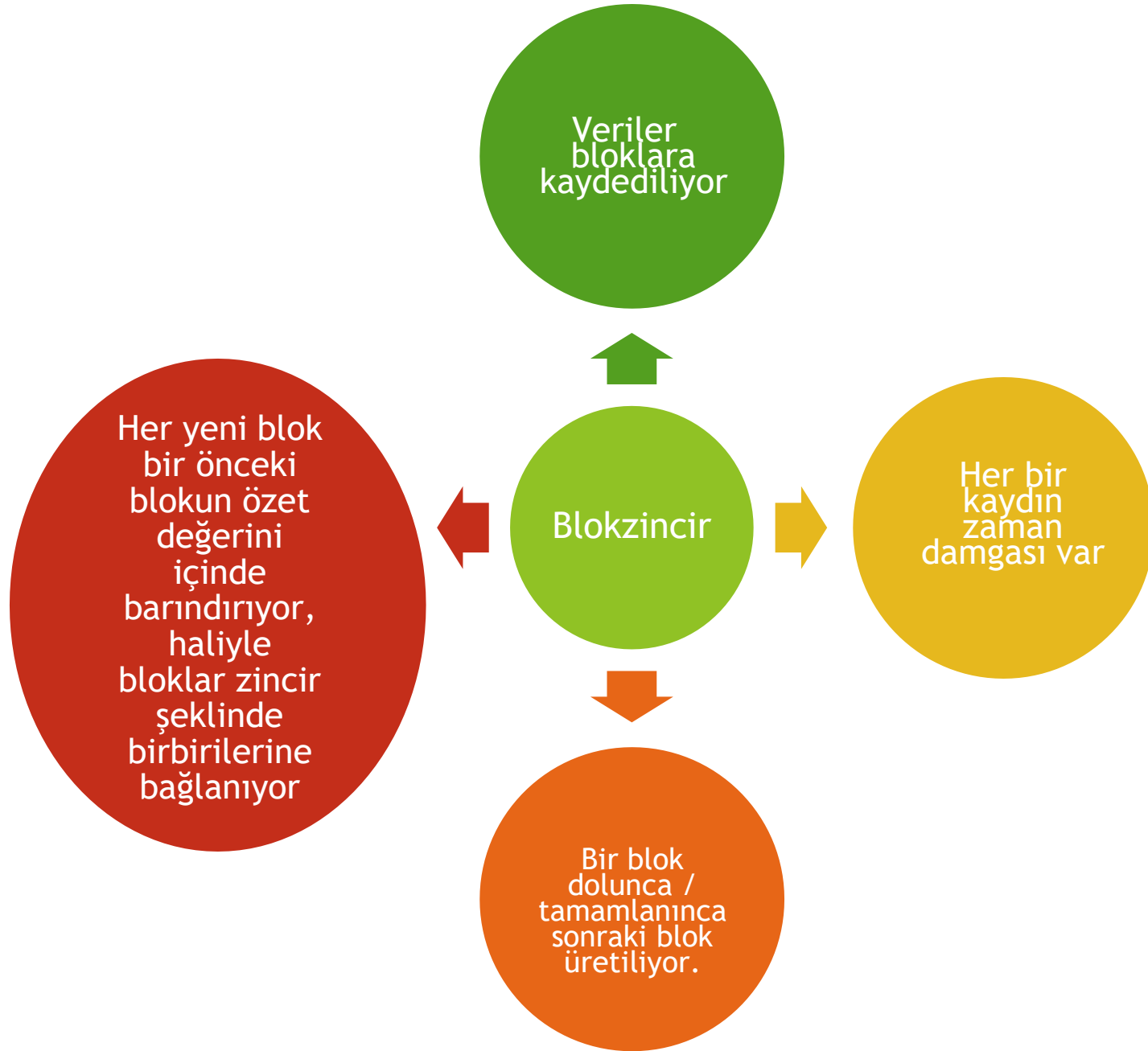
- ▶ Nedir bu Blokzincir?
- ▶ Açık Anahtar / Gizli Anahtar
- ▶ Hash (*Özet değer, Parmak izi*)
- ▶ Blokzincir ile kayıt sistemi
- ▶ Blok yapısı
- ▶ Blok Başlığı
- ▶ Blokzincir’de Güvenlik
- ▶ Çatallanma (*Forking*)
- ▶ Öksüz Blok derken?
- ▶ Dağıtık Kayıt Sistemi (*Distributed Ledger*)
- ▶ İş ispatı (*Proof of Work*) - Pay İspatı (*Proof of stake*)
- ▶ Blokzincir Türleri
- ▶ Blokzincir Teknolojisinden Etkilenecek Konular

Dersin Sorumlusu: Öğr. Gör. Olcay YILMAZ

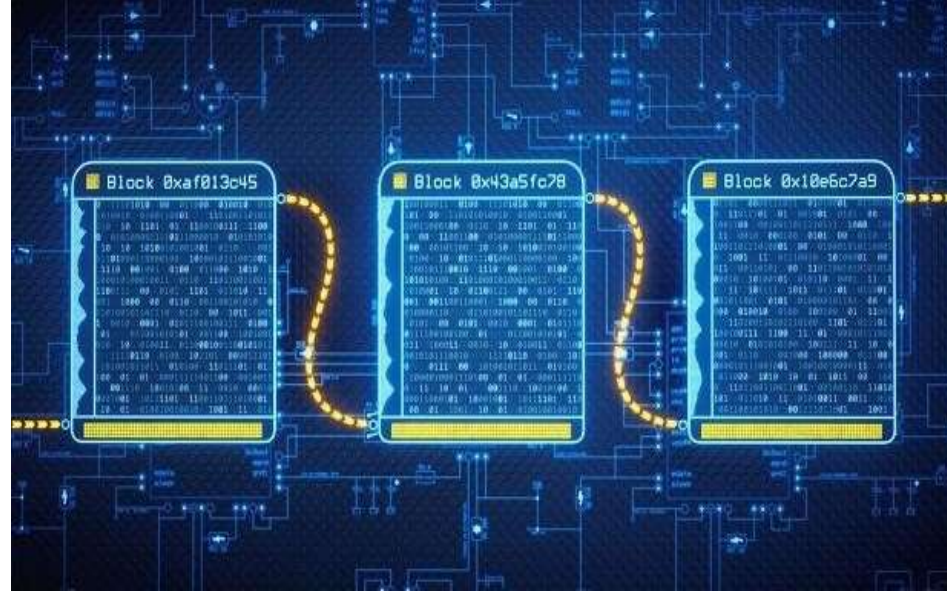
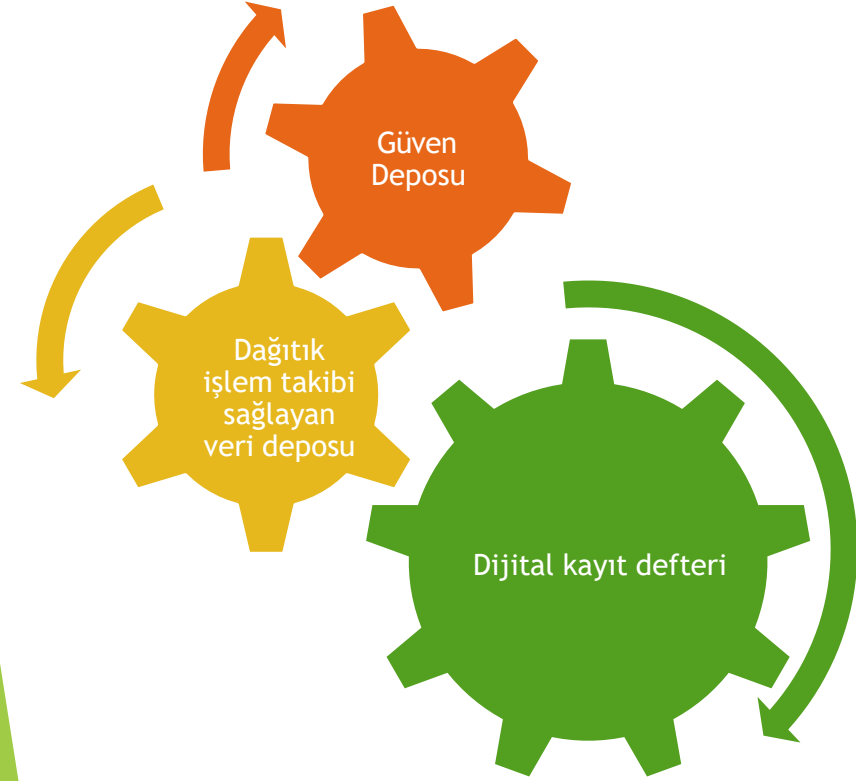
Kaynak: Vedat Güven, Erkin Şahinöz. Blokzincir, Kripto Paralar, Bitcoin, 2018.

Nedir Bu Blokzincir?





Blokszincir



Dünya Ekonomik Forumu Blokszincir Tanımı: Bir aracıya ihtiyaç duymadan, bir verinin iki parti arasında değiş tokuşunu mümkün kılan teknoloji protokolüdür. Ağdaki taraflar şifreli kimlikleriyle anonimce işlemleri gerçekleştirirken, her bir işlem değiştirilemeyen işlem zincirine eklenir ve ağdaki tüm kullanıcılara dağıtılır!

Açık anahtar / Gizli Anahtar

Bilgi Dünyasında Güvenliğin İki Boyutu



Gizlilik (*Bilginin
Şifrelenmesi – Açık
anahtar
kullanımı*)

Doğruluk (*Dijital
imza – Özel
anahtar kullanımı*)

Açık ve gizli anahtar çiftine örnek

- + Örneğin, göndereceğimiz bir bilginin «gizli ve değiştirilmeden» iletilmesini istiyoruz.
Karşı taraftan hangi anahtarı talep ederiz?
 - **Açık anahtar talep ederiz. (Karşı tarafın adresidir bu – Iban gibi düşünelim)**
- + Bu açık anahtar ile bilgi şifrelenip gönderilirken, karşı taraf özel anahtarı ile bu şifreyi çözer, bilgileri okur.
 - **Dijital imzada ise, bilgi doğrulanması ve teyit edilmesinden ötürü özel anahtar ile şifrelenir karşı tarafa açık anahtar gönderilir.**
- + Karşı taraf açık anahtar ile şifreyi çözebiliyorsa, belgenin gönderen tarafından geldiğine emin olur.

Açık ve gizli anahtar çiftine Postacı örneği

*Yaşadığınız apartman giriş şifresi 123** ve posta kutusu numaranız 12 olsun. Size özel bir şey gelmesini ve kimse tarafından okunmamasını istiyorsunuz. Postacıya ne verirsiniz?*



Apartman giriş şifresi ve posta kodunu yani açık anahtarınızı verirsiniz. Postacı açık anahtarınız ile apartmana girer, posta kutunuza erişir fakat içeri açamaz. Posta kutunuza dosyayı bırakır. Siz özel anahtarınız ile posta kutunuzu açar belgeyi okursunuz.

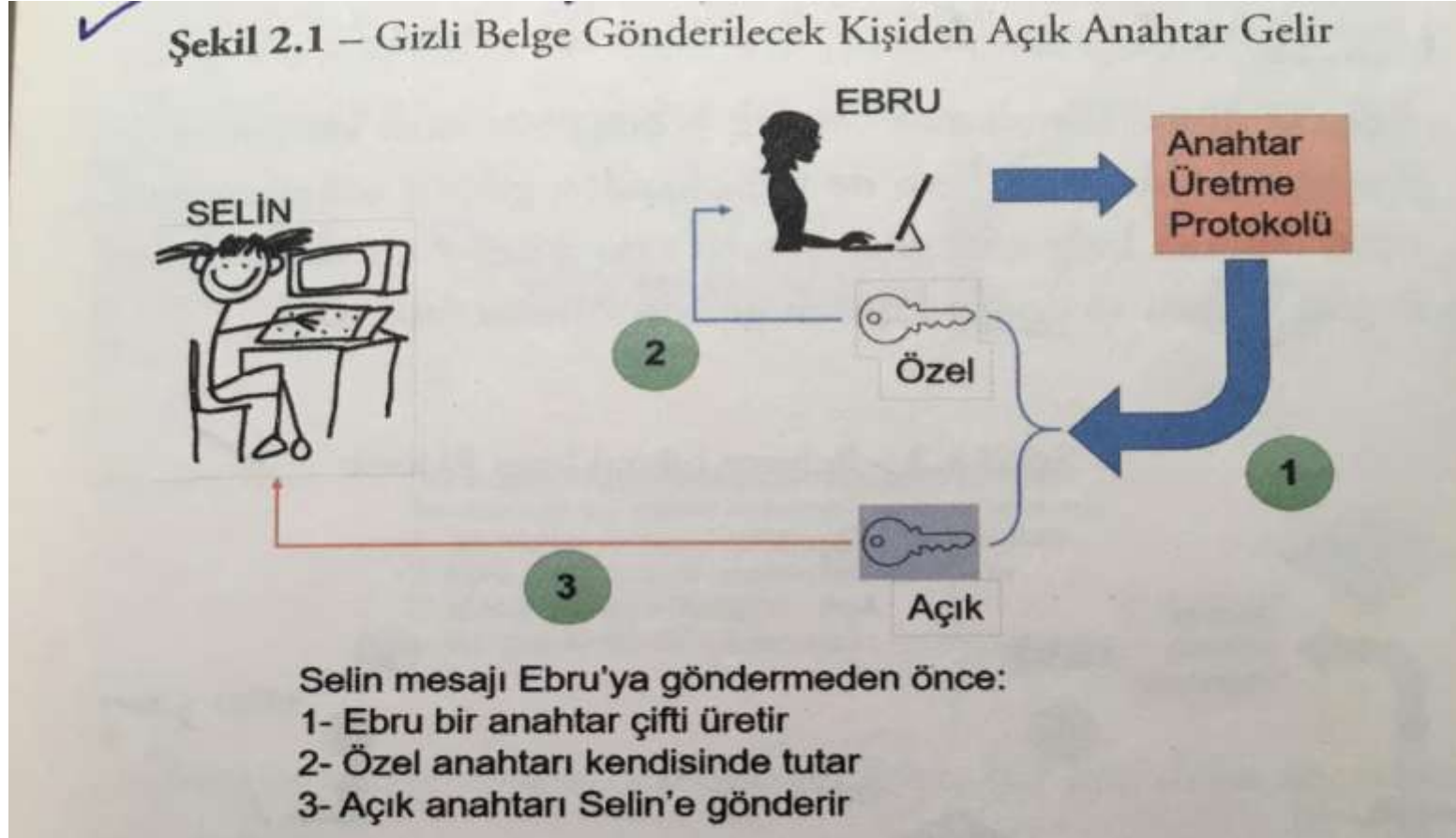
Diğer senaryoda, gönderilecek bilginin görülmesinde sakınca yok. Sadece gönderenin belli olmasını istiyorsunuz. (Doğrulama, teyit, dijital imza)



Özel anahtarınız ile posta kutunuzu açıp belgeyi içine koyar ve posta kutunuzun kapağını açık bırakırsınız. Postacıya açık anahtarınızı verirsiniz. Postacı açık anahtarınız ile apartmana girer, posta kutu numaranızın önüne gelir. Kutu açık olduğu için bunun sizin tarafınızdan geldiğini teyit etmiş olur.

Açık ve gizli anahtar çiftine uygulamalı örnek

Gizli bir belge göndermek

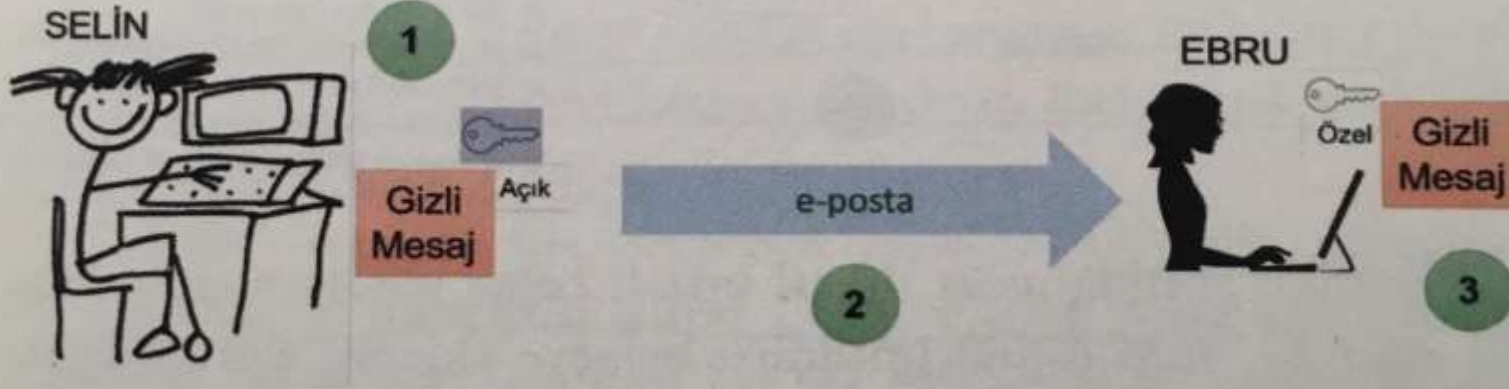


Açık ve gizli anahtar çiftine uygulamalı örnek

Gizli bir belge göndermek

Artık Selin, gizli mesajını Ebru'ya göndermeye hazırdır.

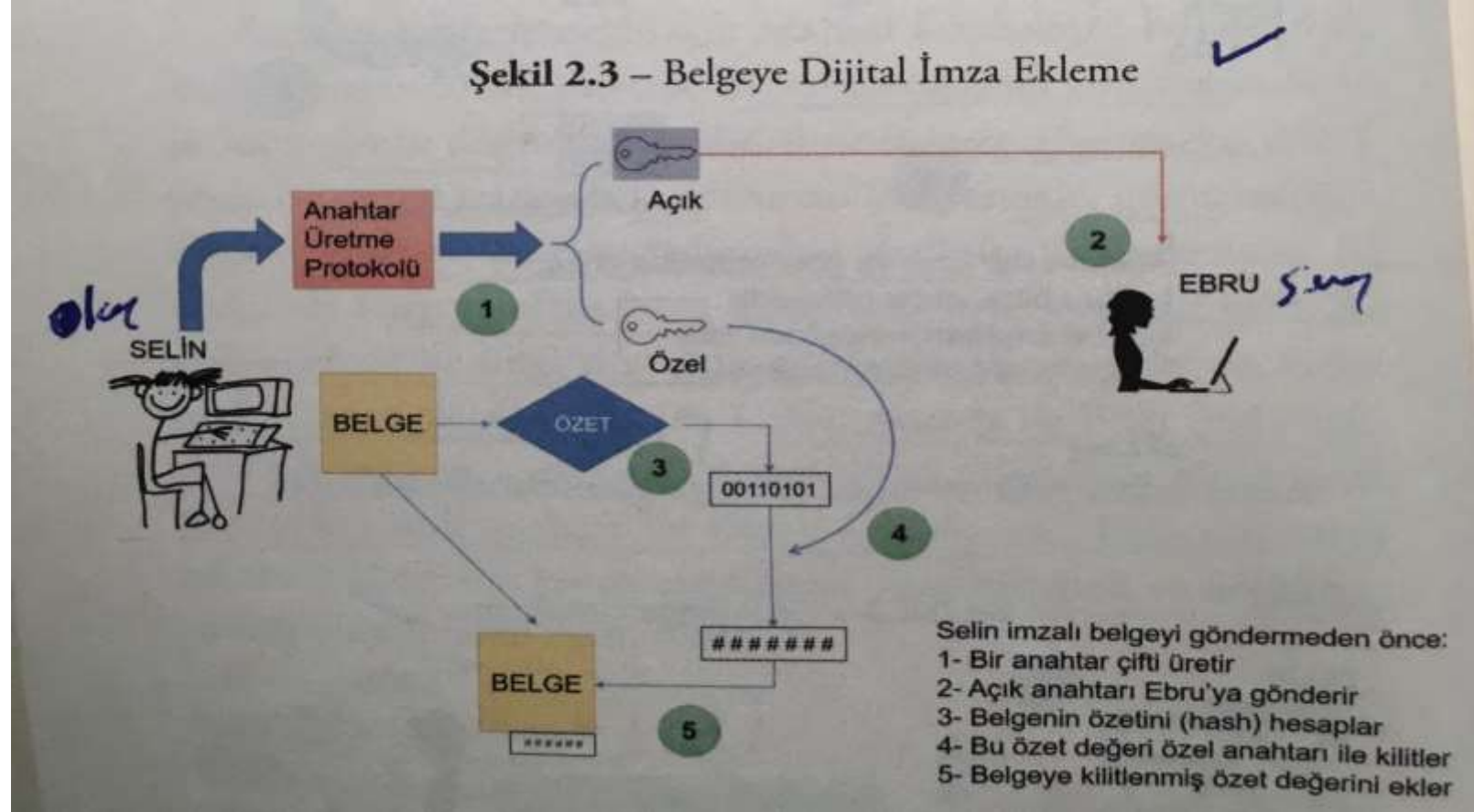
Şekil 2.2 – Gizli Belge Gönderme ✓



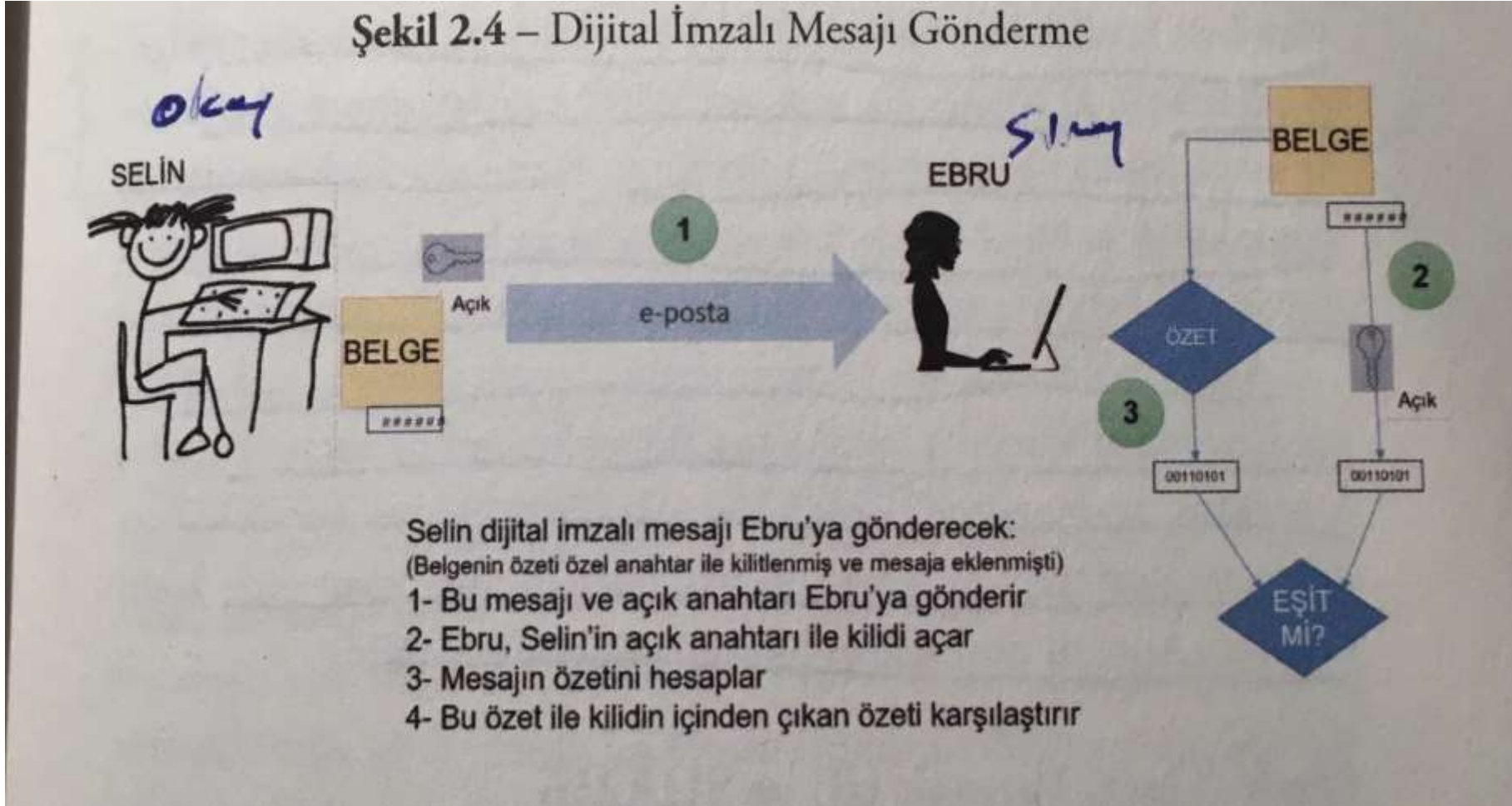
- Selin mesajı Ebru'ya göndermek için:
- 1- Mesajını Ebru'nun açık anahtarı ile şifreler
 - 2- Bu mesajı Ebru'ya gönderir
 - 3- Ebru, özel anahtarı ile kilidi açar

Açık ve gizli anahtar çiftine uygulamalı örnek

Belgeyi doğrulama - Dijital İmzalama



Açık ve gizli anahtar çiftine uygulamalı örnek *Belgeyi doğrulama - Dijital İmzalama*

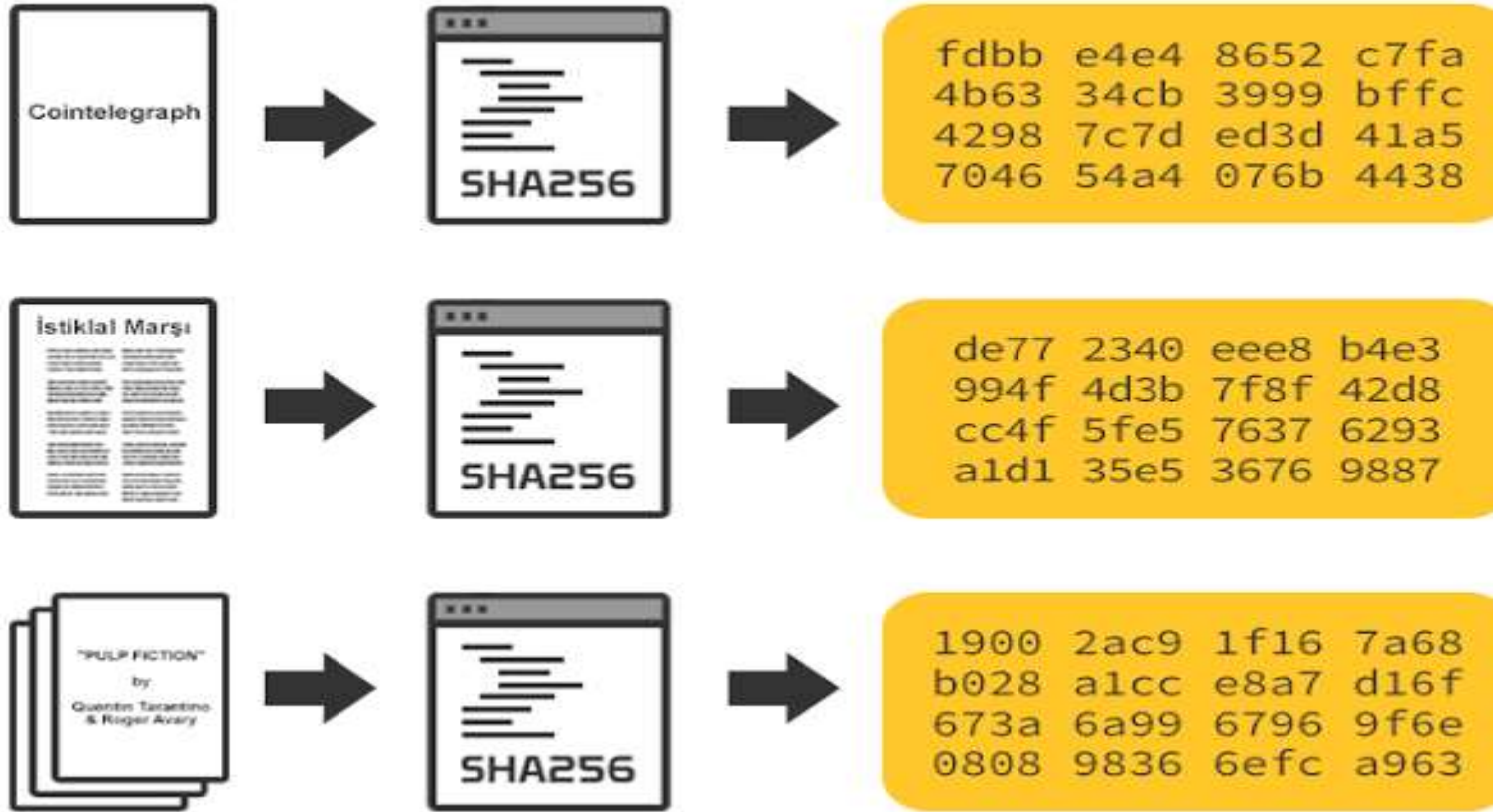


Hash (Özet değer - Parmak izi)



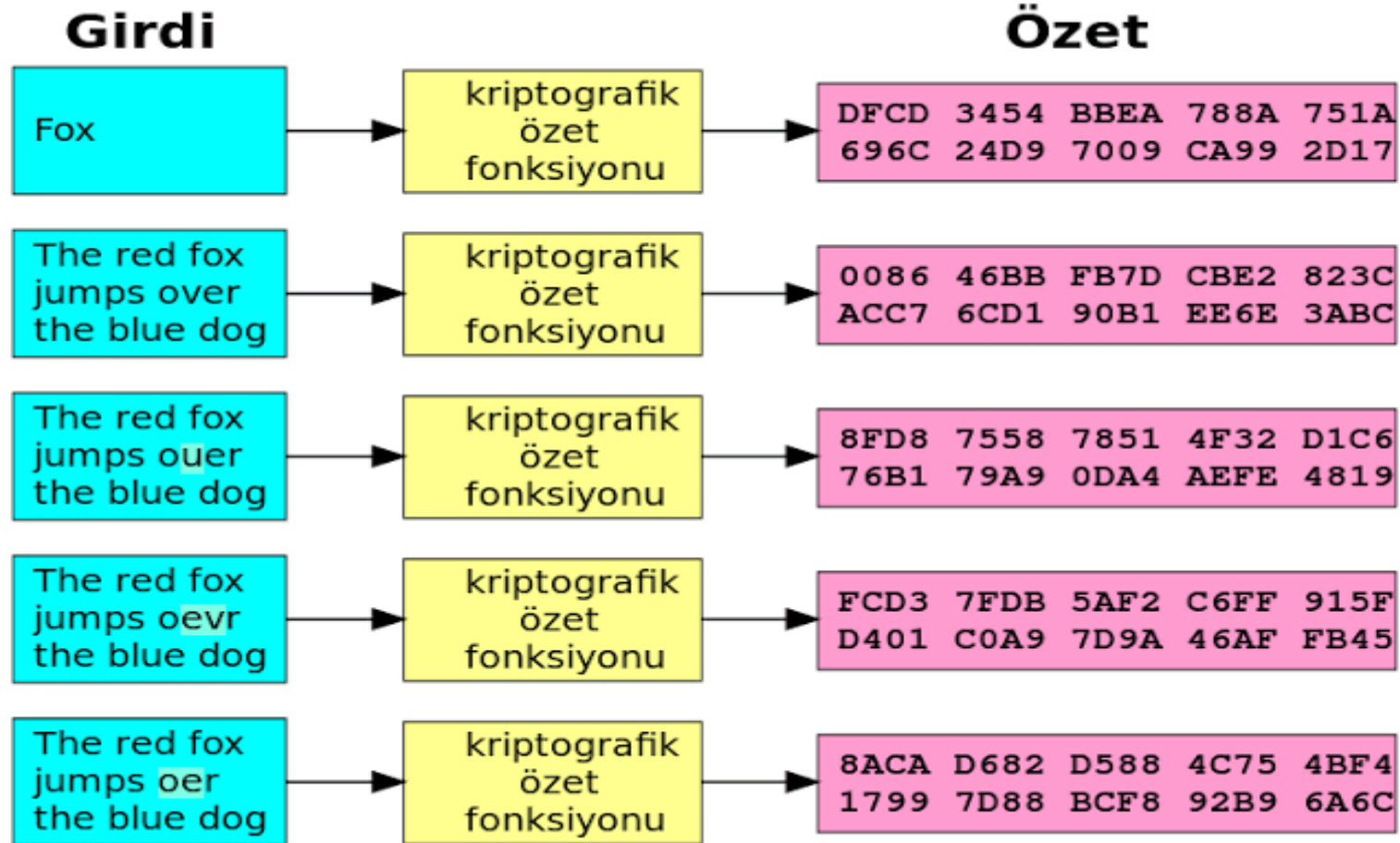
Hash Örnekleri (Özet değer - Parmak izi)

SHA256 HASH ALGORİTMASI ÖRNEĞİ



Kaynak: <https://tr.cointelegraph.com/news/what-is-hash-whats-the-meaning-of-bitcoin-sha-256-algorithm>

Hash Örnekleri (Özet değer - Parmak izi)



Kaynak: <https://www.bilimcag.com/nedir/hash-fonksiyonu-ozetleme-fonksiyonu-nedir/>

Hash Uygulaması (Özet değer - Parmak izi)

Blockchain Demo

Hash

Block

Blockchain

Distributed

Tokens

Coinbase

Advanced ▾

Enable Expert Mode

SHA256 Hash

Explanation

Input:

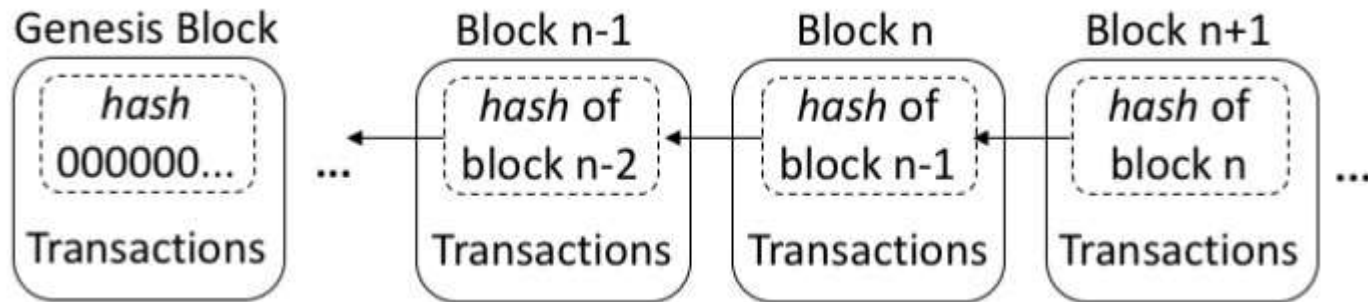
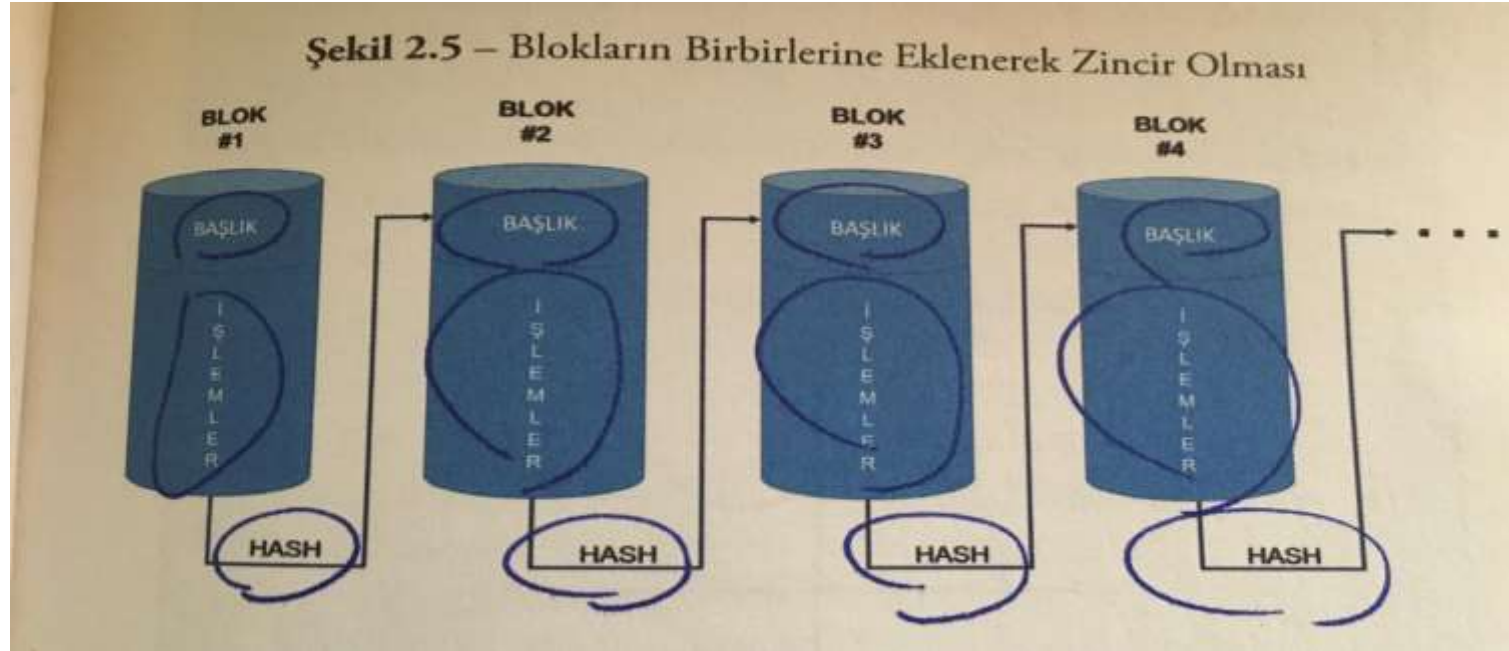
Olca YILMAZ

Hash:

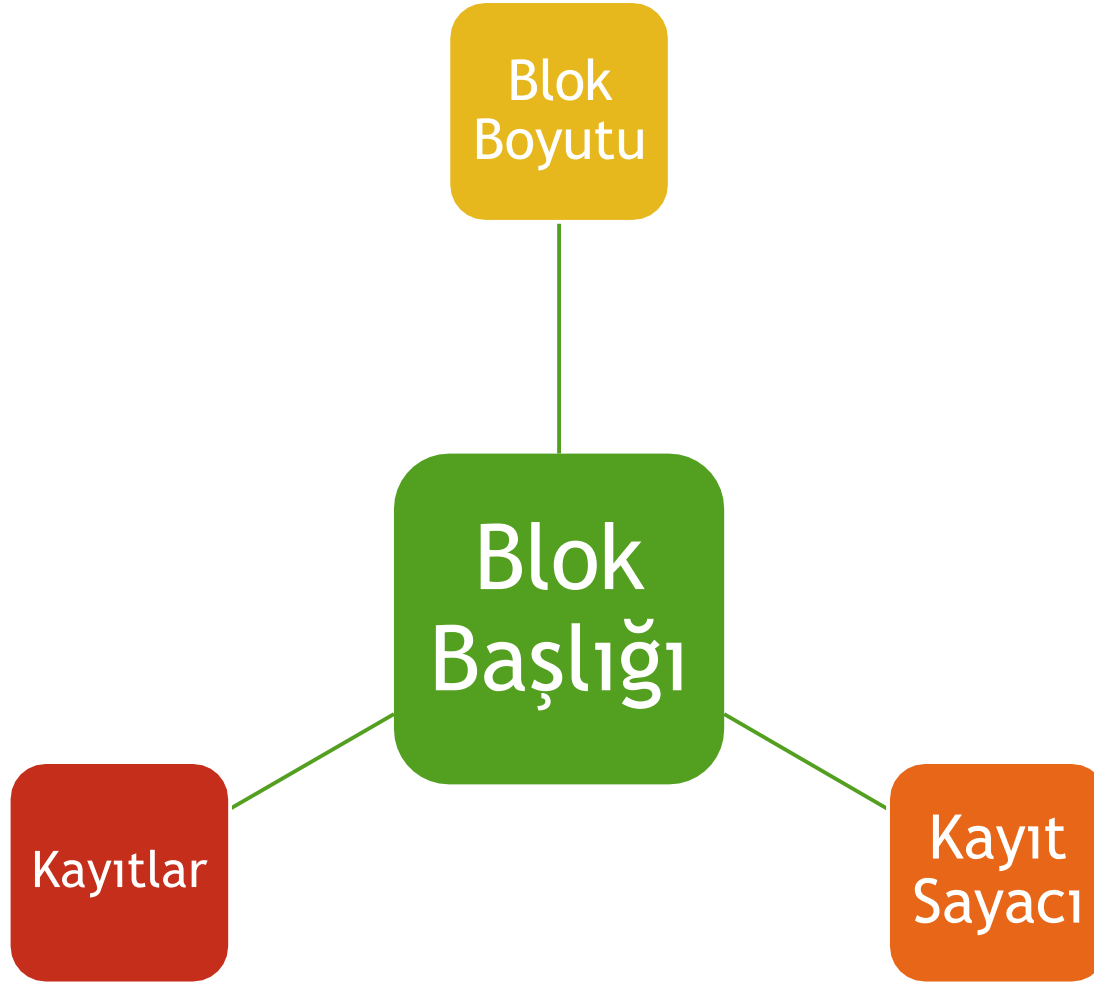
fca7cccd1208411d114114ccb6f589aca4adc7058b467ccf68ec089c8f9aada9

Kaynak: <https://guggero.github.io/blockchain-demo/#!/hash>

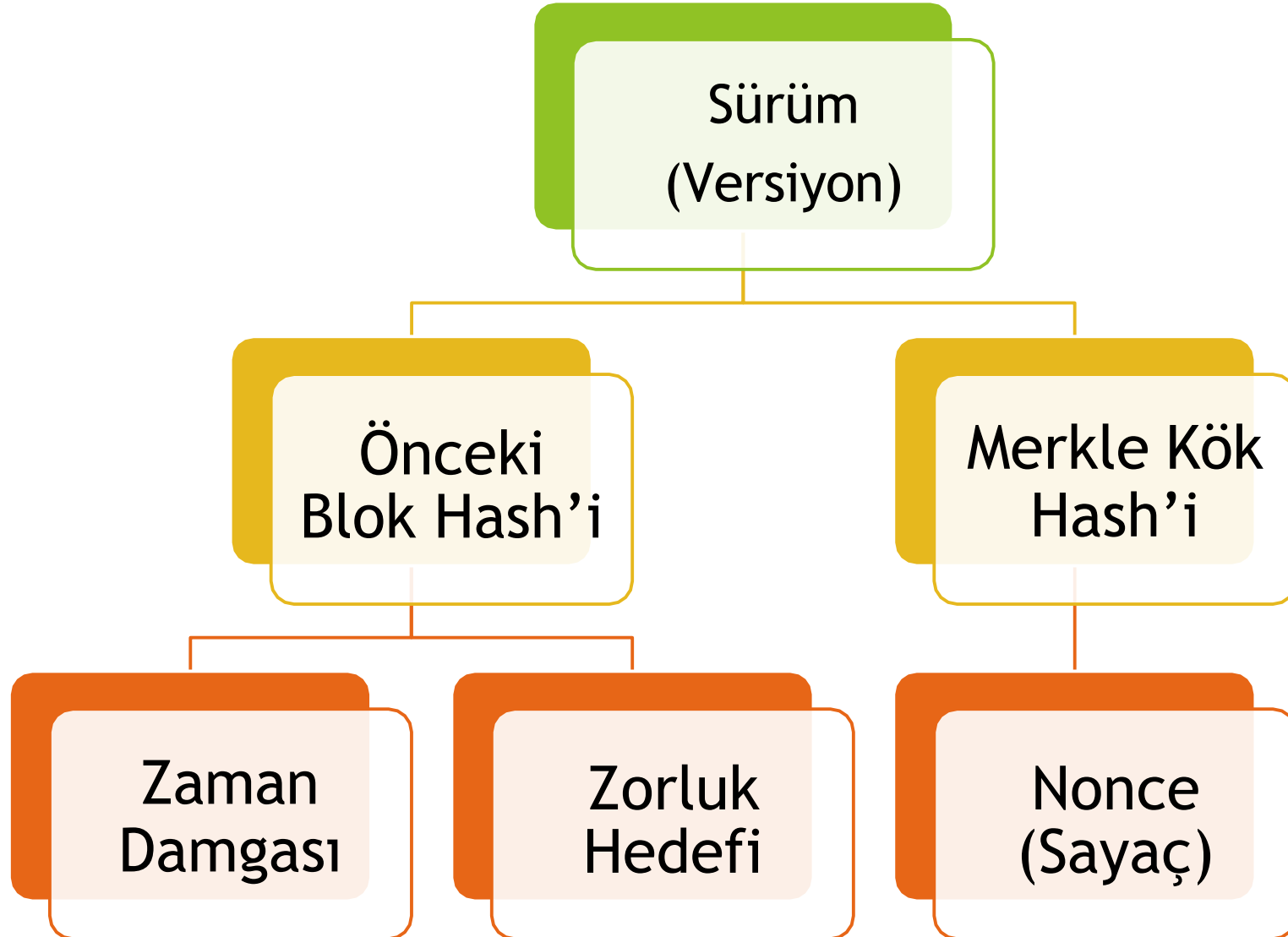
Blokzincir ile Kayıt Sistemi



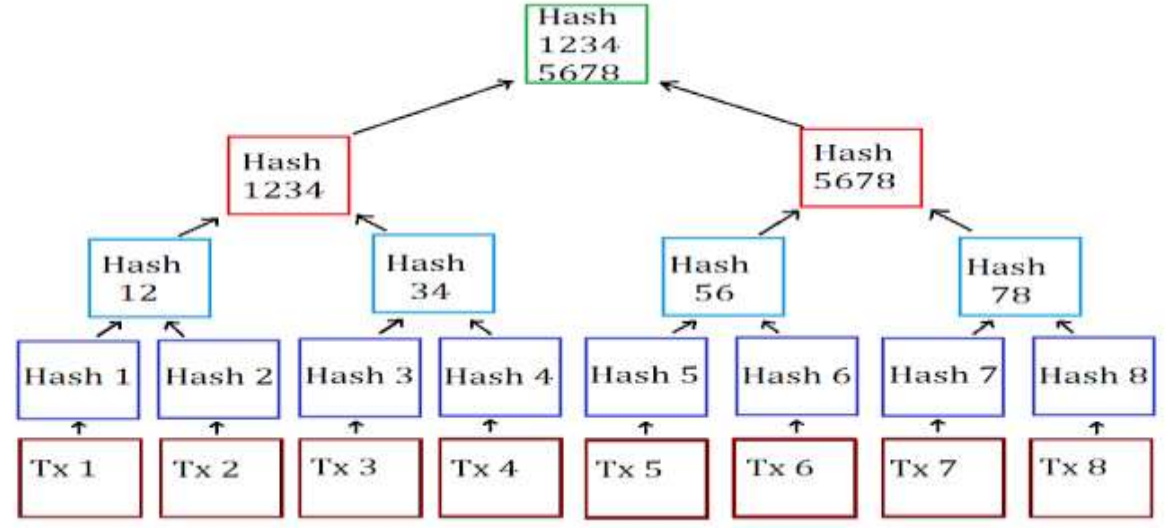
Blok Yapısı



Blok Başlığı

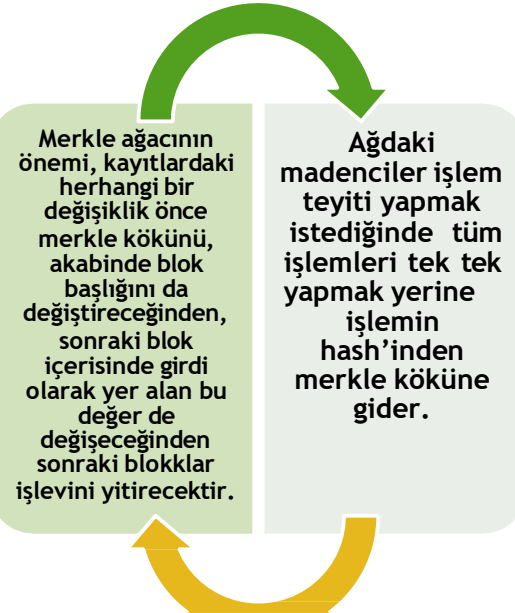


Merkle Ağacı ve Merkle Kökü

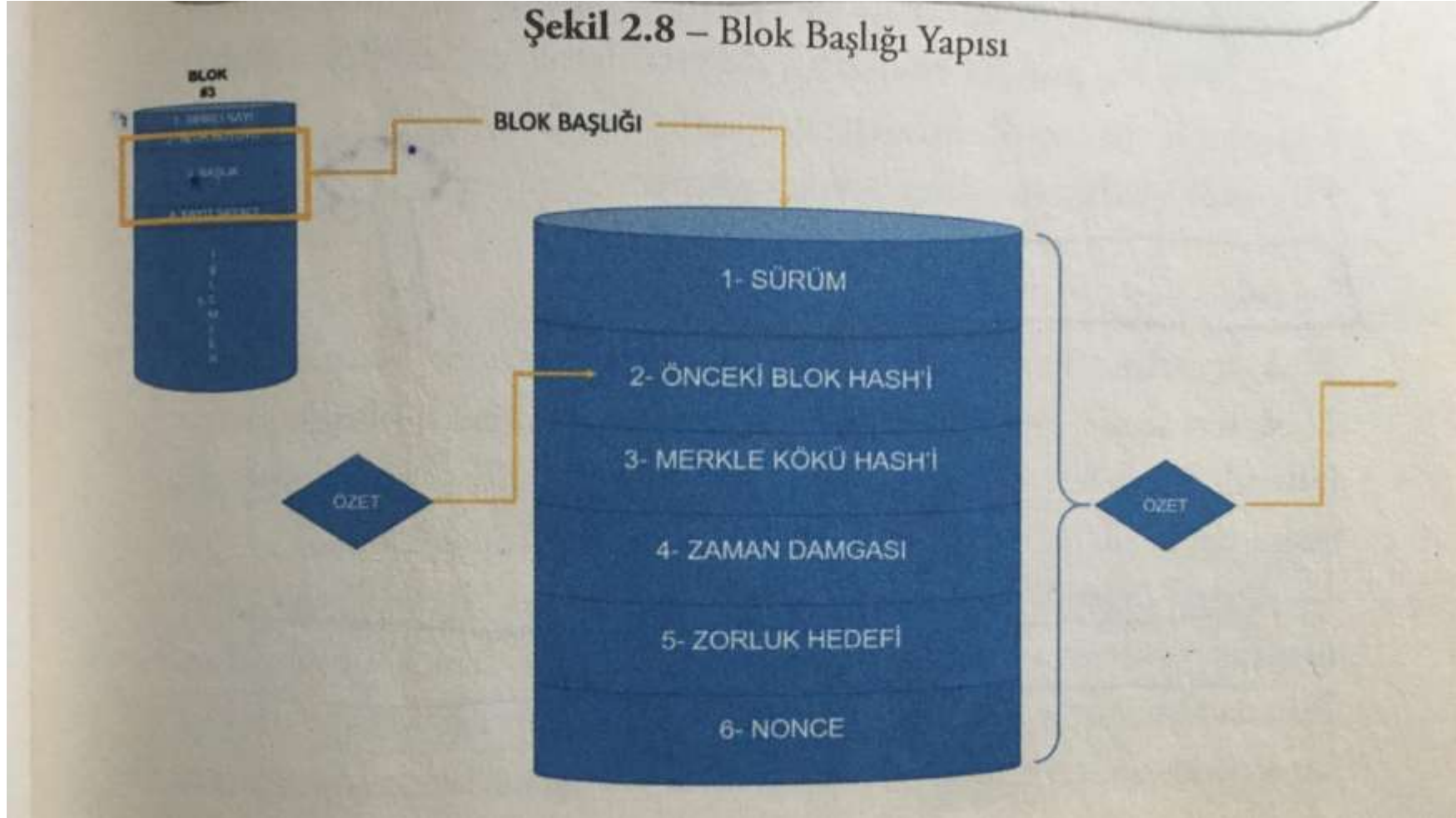


Kaynak: <https://kursataelf.medium.com/merkle-a%C4%9Fac%C4%B1-merkle-tree-nedir-ve-neden-kullan%C4%B1%C4%B1r-e57583fab8a1>

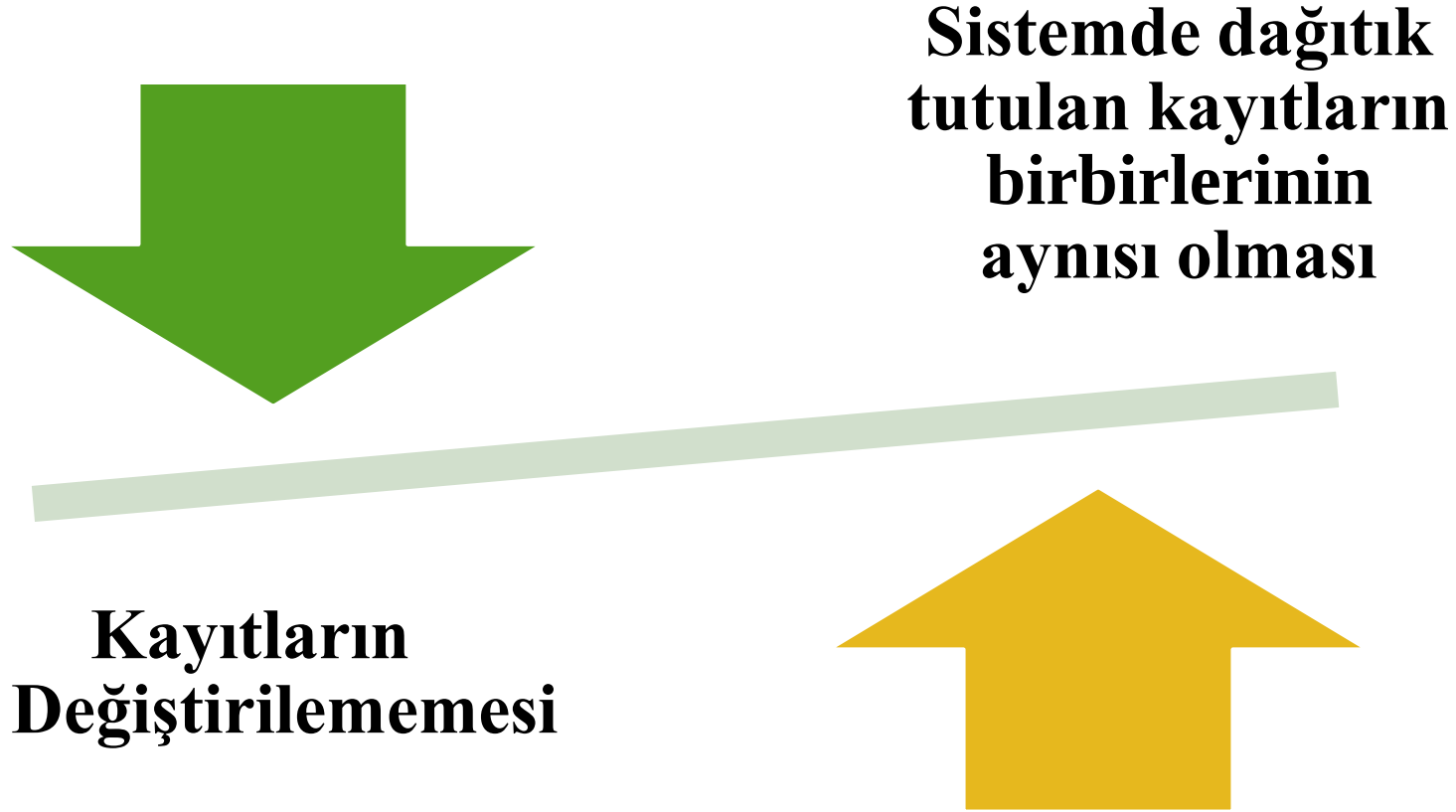
Kaynak: <https://changelly.com/blog/merkle-tree-explain/>



Blok yapısından Blok Başlığına



Blokzincir'de Güvenlik



Geçmiş Bir kaydın Değiştirilmesi / Hacklenmesi Örneği

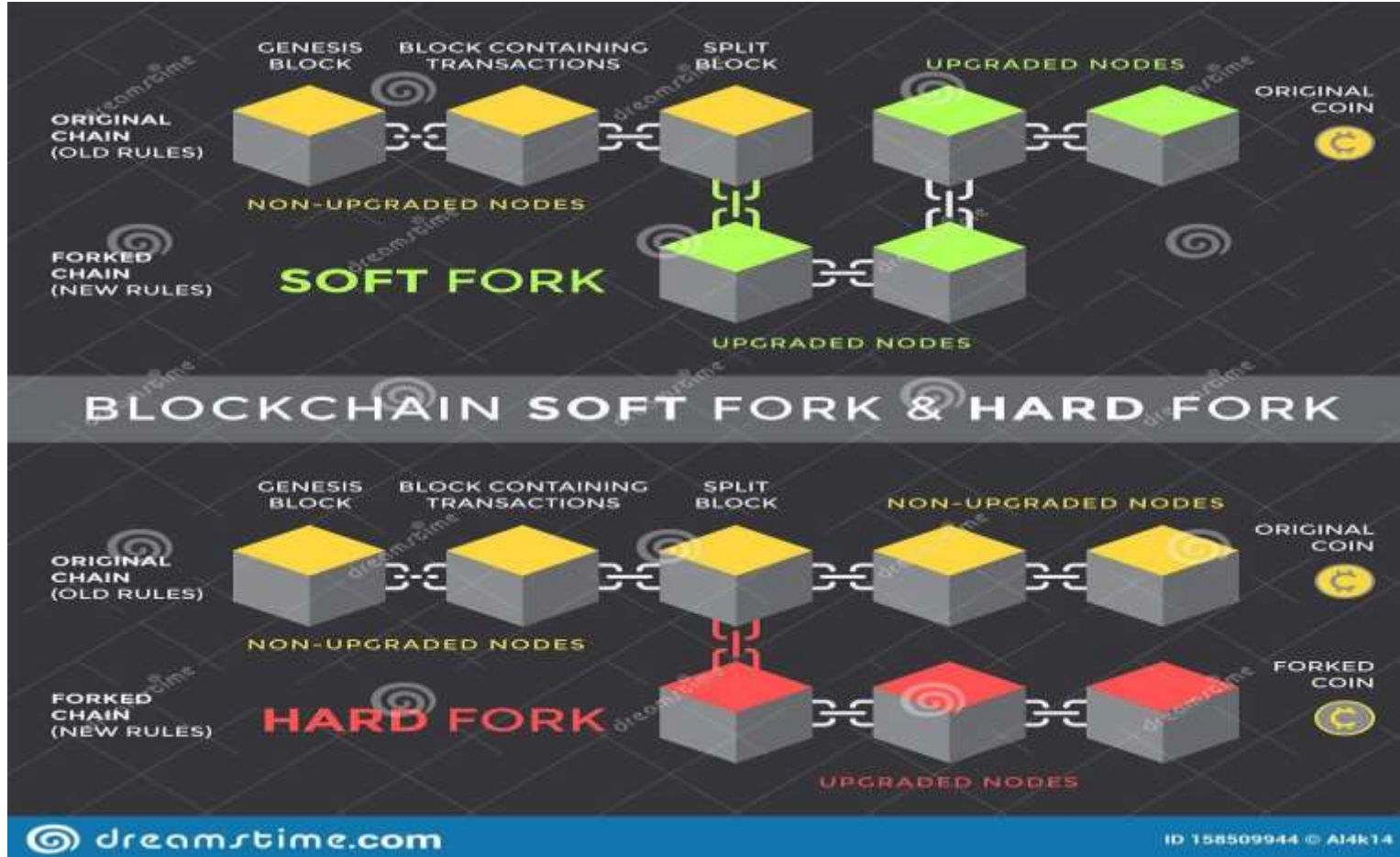
Bir kaydı, işlemi değiştirmeye yeltenen kötü niyetli kullanıcı ilgili blokun hash değerinin değişmesine neden olacaktır.

An itibariyle 750 bininci blok oluşuyor olsun (her 10 dakikada yeni bir blok sisteme dahil oluyor) 620 bininci bloku değiştiren kullanıcı, bu blokun hash değerinin ve sırasıyla bu bloktan sonra üretilen blok özetlerinin de değişmesine sebep olacaktır.

Bu noktada ağdaki tüm madenciler aynı verilere sahiptir ve madencilerin önüne iki farklı zincir gelirse, madenciler uzun olan zinciri kabul edip yoluna devam edecektir. Kötü niyeti kullanıcı ise sistemden ret yiyecektir.

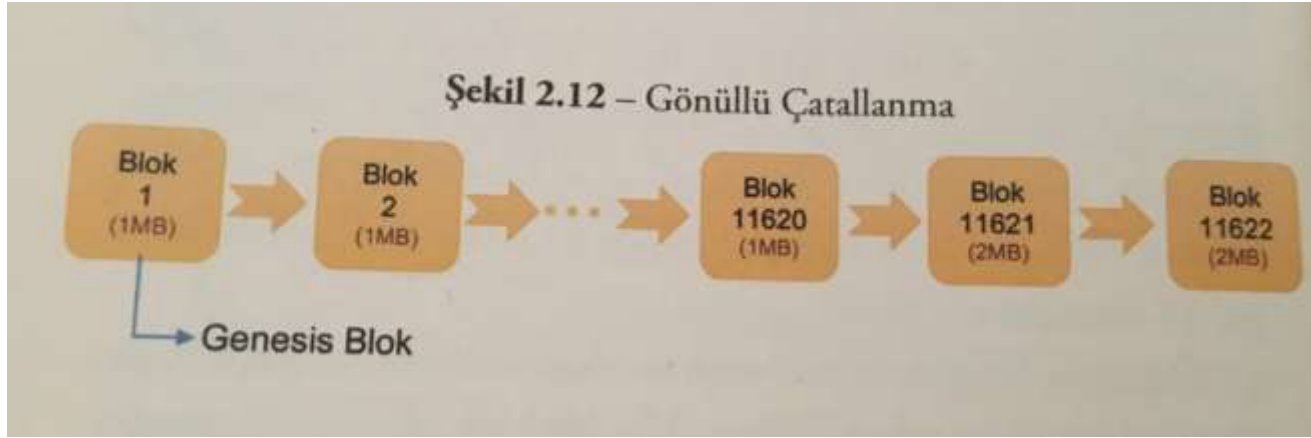
Çatallanma / Forking

Ağdaki madencilerin konsensüsü, mutabakatı ile yürüyen blokzincir teknolojisinde zaman içerisinde blok yapısında var olan kurallarda revizyonlar gerekebilir. Bkz: Blok boyutunun artması, problem zorluk derecesinin düşürülmesi gibi.

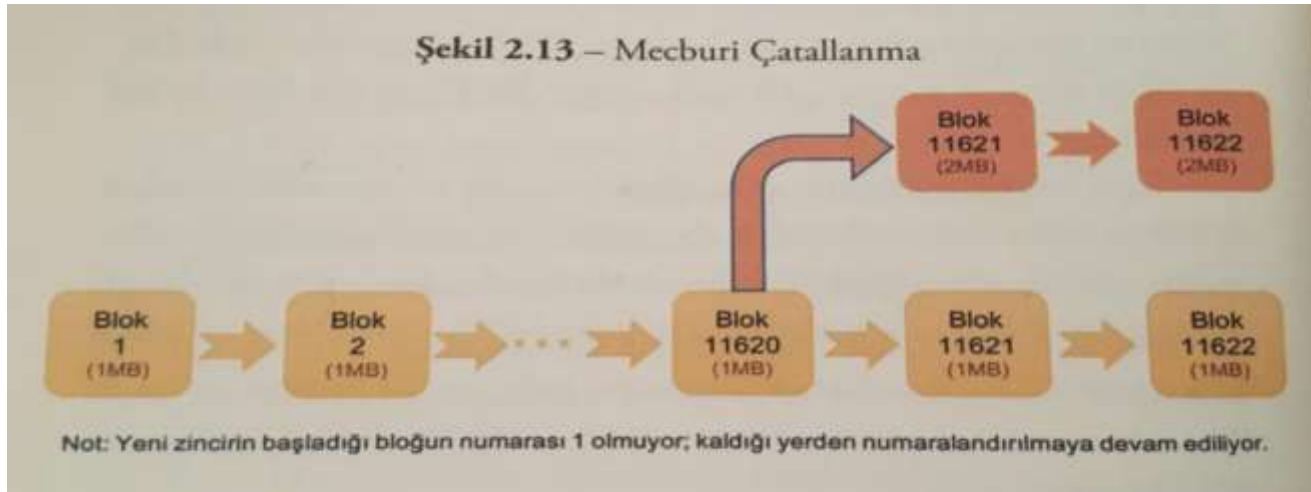


Çatallanma / Forking Örnekleri

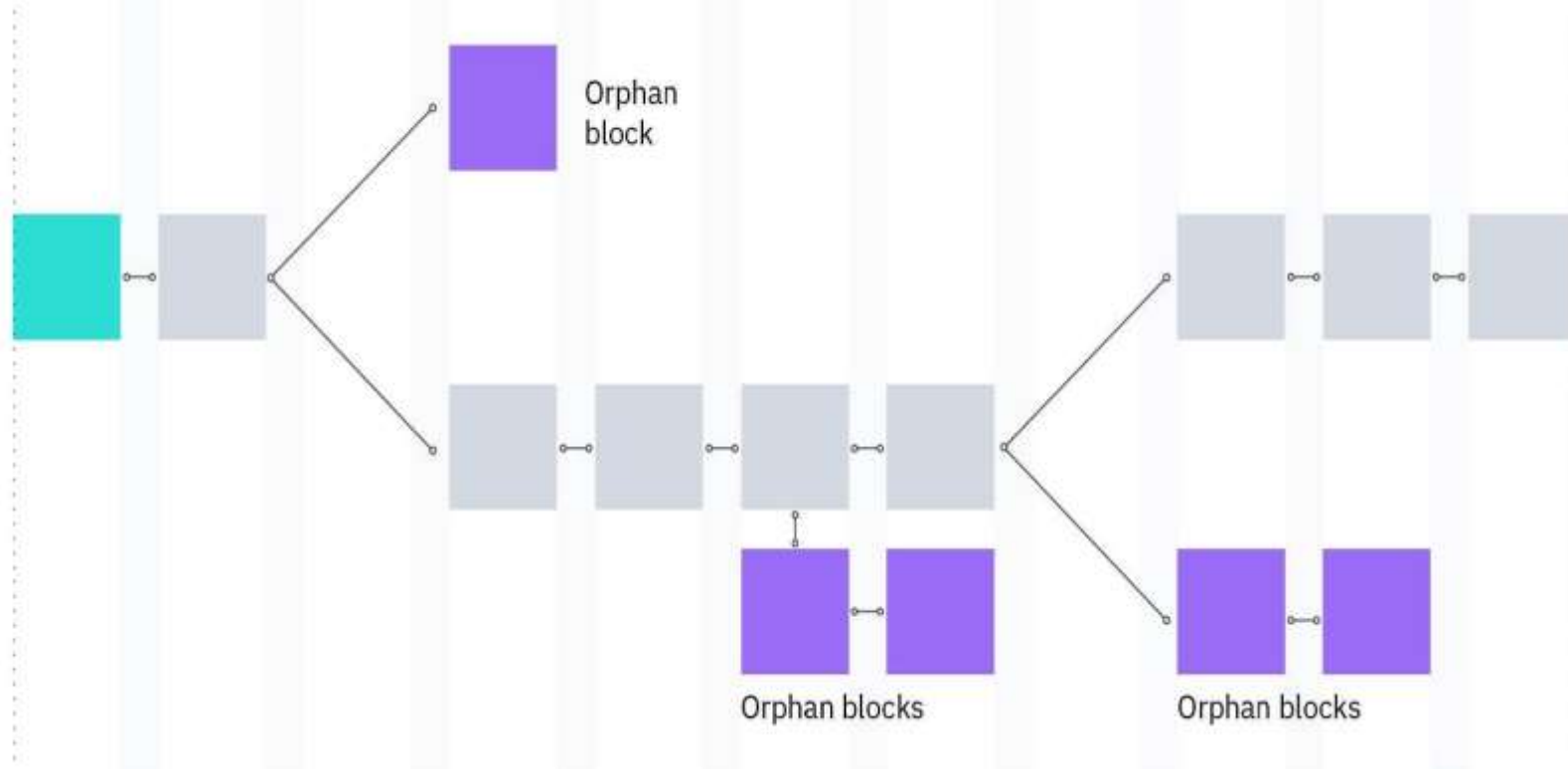
► Gönüllü Çatallanma



► Mecburi Çatallanma



Öksüz Blok (Orphan Block)



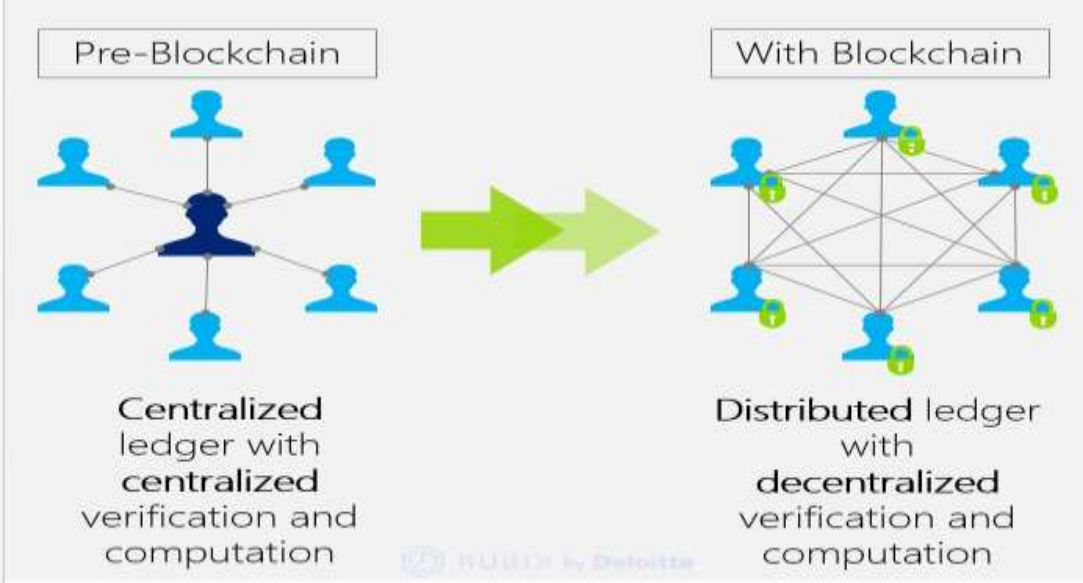
Kaynak: <https://filecoin.io/blog/tipsets-family-based-approach-to-consensus/>

Öksüz blokun içerisindeki işlemlere ne oluyor? Peki ya Blok üretilmesiyle kazanılan ödüller?

Öksüz blok içerisindeki işlemler tekrar işlem havuzuna bırakılır. İşlem teyidi için en net güvence *3,4 blok daha üretilmesi* şeklindedir.

Her Madenci ürettiği blok için **ödül + komisyon** kazansa da bu ödülü 19 blok boyunca (190 dk) harcayamaz. 3,4 madenci bu tutarı kazansa da, **gerçek ödül sahibi 19 blok sonra netleşir.**

Dağıtık Kayıt Sistemi (Distributed Ledger)

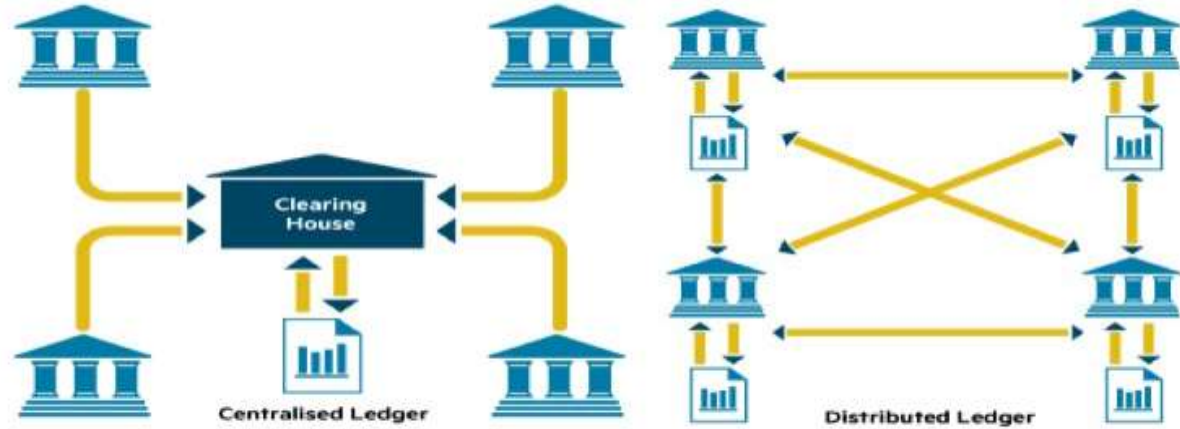


Not: İşlemleri gerçekleştiren taraflar arasında bir güven sorunu yoksa yahut işlemlerin kaydını tutan, teyidini sağlayan bir merkezi otorite varsa dağıtık kayıt sistemine gerek olmaz.

Not: Blokzincir de bir dağıtık kayıt sistemidir.
Taraflar birbirini tanısin, tanımasını birbirlerine güven duymaları gerekmeden karşılıklı işlem gerçekleştirebilirler.

Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

Proof of Work (POW) / Proof of Stake (POS)

İş İspatı

/

Pay İspatı

Her iki yöntem de, madencilerin her saniye blok üretmelerini engellemek amacıyla blok üretimlerinin belirli aralıklarla olmasını sağlamak maksatlı ortaya atılmış **MUTABAKAT algoritmalarıdır.**

Hani kuralları baştan çizili olan platformların altyapısını oluşturan blokzincir teknolojisinde blok üretiminde bulunmaları ve bloğun hash değerini çözümlemeleri için sistem bir problem veriyor ya madencilere.. Blok özetini bul, hesapla, kanıtlar diyor.. **İşte POW ve POS bu..**



Proof of Work



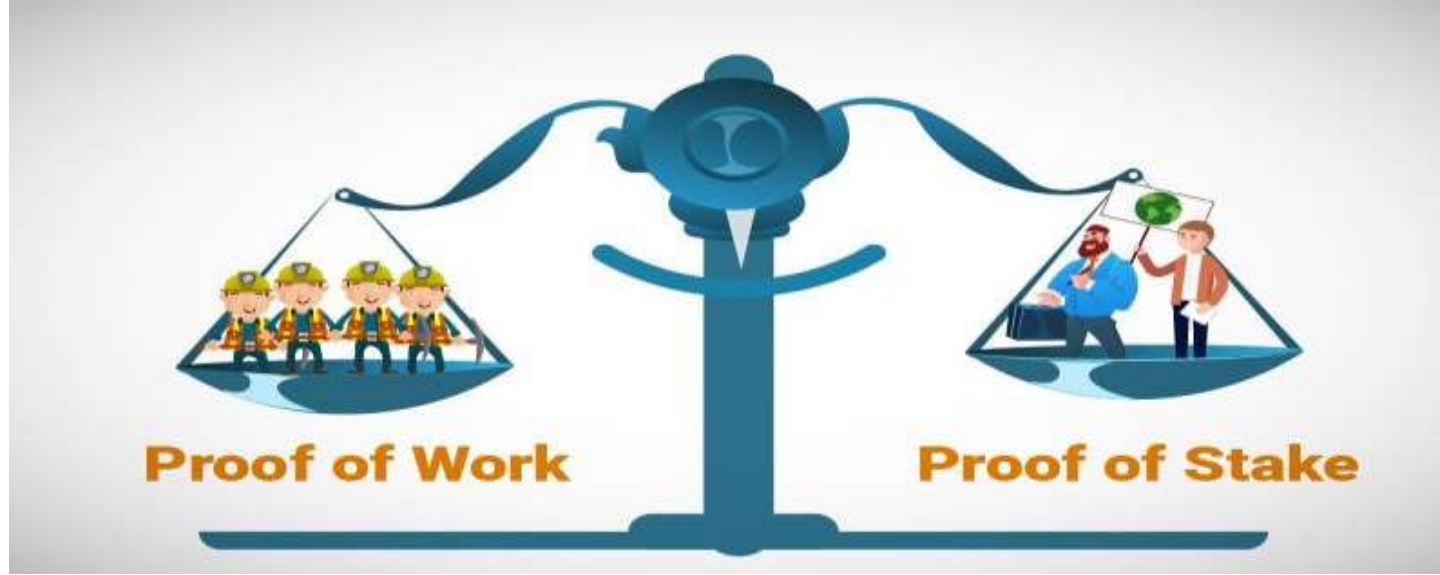
Proof of Stake

Proof of Work (POW) / Proof of Stake (POS)

İş İspatı

/

Pay İspatı

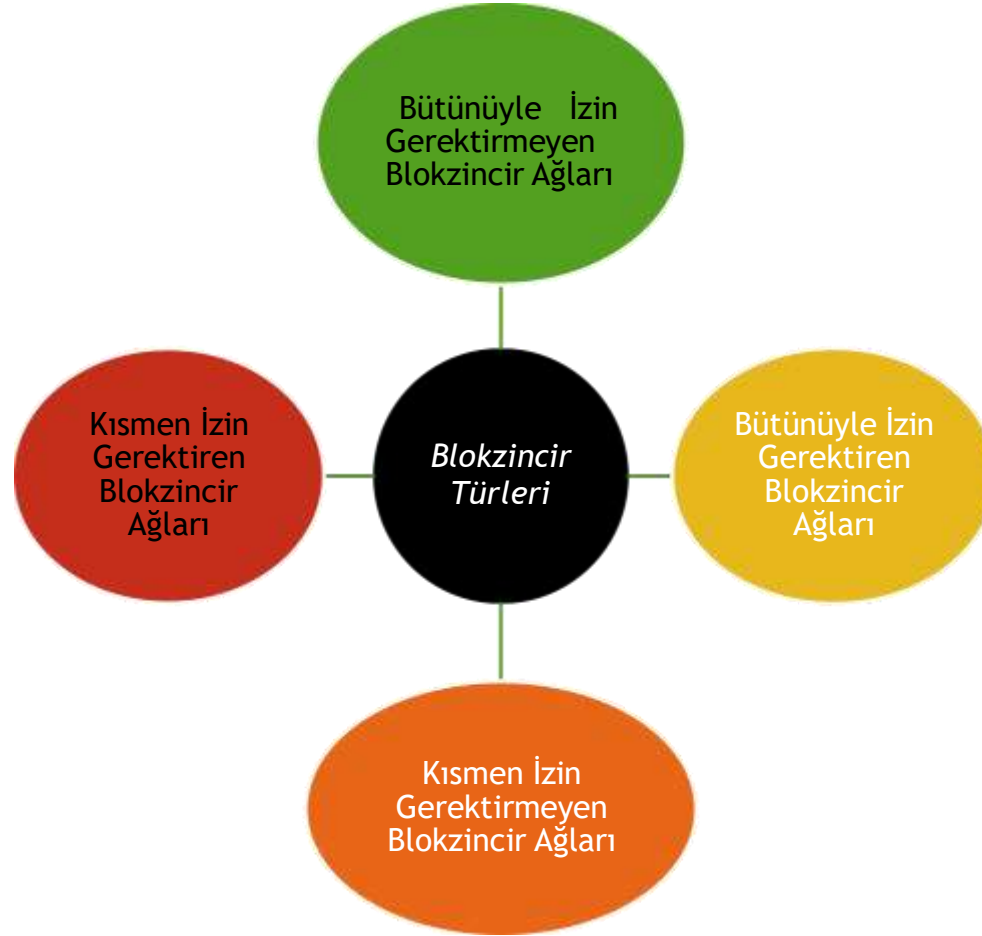


Kaynak: <https://www.skalex.io/proof-of-work-vs-proof-of-stake/>

Not: POW Bitcoin blokzinciri içerisinde madencilerin ispatla yükümlü oldukları algoritmalar iken, POS ise Ethereum (akıllı sözleşmeler) blokzincirinde madencilerin yarış içerisine girmeyip, ne kadar fazla paya (ether'e) sahip ise blok oluşturma görevinin kendisine verilmesi şeklinde çalışmaktadır bu dönem itibariyle. (bkz: *Ethereum 2.0*)

POS'da ödül yoktur, komisyon vardır. POS'un POW'a göre artıları: **Enerji tüketimi daha az iken**, eksileri: **Ether payına daha çok sahip olan madencilerin blok üretme şansının daha çok olması** şeklindedir.

Blokzincir Türleri



Tür 1: Bütünüyle İzin Gerektirmeyen Blokzincir Ağları (Açık-Public)

- Eğer bir Blokzincir ağına girerek kayıtlı verileri okumak için izin almanız gerekmiyorsa ve bu ağın “mutabakat yapısına” uyarak, yeni bloklar ekleyebilmek için “mutabakat sürecine” dahil olmak için yine izin gerekmiyorsa, bu tarz ağlara **Bütünüyle İzin Gerektirmeyen Blokzincir Ağları** adı verilir. Bitcoin platformu buna örnektir. Açık kaynak kodludur.

Tür 2: Kısmen İzin Gerektirmeyen Blokzincir Ağları (Açık-Public)

Eğer bir Blokzincir ağına girerek kayıtlı verileri okumak için izin almanız gerekmiyorsa ama bu ağın “mutabakat yapısına” uyarak yeni bloklar eklemek ve “mutabakat sürecine” dahil olmak için izin gerekiyorsa, bu tarz ağlara **Kısmen İzin Gerektirmeyen Blokzincir Ağları** adı verilir.

Tür 2: Kısmen İzin Gerektirmeyen Blokzincir Ağlarına Örnek

Şu anda dünya üzerindeki en önemli problemlerden birisi haber kaynaklarının güvenliğidir. Sosyal medya kanallarından akan haberler başta olmak üzere zaman zaman çok büyük haber ajansları bile yanlış olarak hatalı haberler geçebilmektedir. Bu sorunu çözmek için üretilen bir Blockchain Ağı düşünelim. Ağımızın adı “Güvenli Haber Blockchain Ağı” olsun. Bu ağda her bir haber yeni bir blok olarak kaydedilsin ve dileyen herkes bu ağa erişerek haberleri okuyabilsin. Ancak ağa yeni bir haber eklemek için “mutabakat yapısı” resmi bir haber ajansı olmayı gerektirsin. Resmi bir haber ajansı ağa bir haber gönderdiğinde ise bu haberin bağımsız üç farklı haber ajansı tarafından daha onaylanması mecburi olsun (mutabakat süreci) ve bu onaylar gelince haber bir blok olarak ağa eklensin.

Kaynak: Blockchain 101, Ahmet Usta, Serkan Doğantekin

Tür 2: Kısmen İzin Gerektirmeyen Blokzincir Ağlarına Örnek

- *Bir örnek daha verelim: Bağımsız müzisyenlerin parçalarını yayınladıkları bir Blockchain platformu düşünelim. Bu durumda sisteme giren herkes tüm müzik parçalarını dinleyebilir ve bunlara erişebilir. Ancak “mutabakat yapısı” gereği sisteme sadece bağımsız müzisyenlerin parça eklemesine izin verilmektedir. Bu parçaların orijinal ve benzersiz olduğunu ise “mutabakat süreci” gereği meslek birlikleri sağlar. Bu durumda bu ağa erişenlerin çıkarı, müzik parçalarını dinlemek; mutabakatı sağlayanların çıkarı ise eserlerinin kayıt altına alınması (telif ve belki gelir süreçlerini de düşünerek) olur.*

Kaynak: Blockchain 101, Ahmet Usta, Serkan Doğantekin

Tür 3: Kısmen İzin Gerektiren Blokzincir Ağları (Özel-Private)

- Eğer bir Blokzincir ağına girerek kayıtlı verileri okumak için izin almamız gerekiyorsa ama sonrasında bu ağın “mutabakat yapısına” uyarak yeni bloklar eklemek ve “mutabakat sürecine” dahil olmak için izin gerekmiyorsa, bu tarz ağlara **Kısmen İzin Gerektiren Blokzincir Ağları** adı verilir.

Bir bankanın kendi şubeleri arasında gerçekleşen havale sistemi için örnek verilebilir. Bir bankanın şubeleri arasındaki havale işlemlerini tutmak ve bu bankaya özel bir Blokzincir ağına erişmek için, Bankanın bir şubesi olmak mecburi olacaktır. Ancak bir şube içeriye giriş yaptıktan sonra artık “mutabakat yapısı” ve “mutabakat sürecine” dahil olacaktır. Böylece herhangi bir şubenin veya bir grup şubenin tüm sistemleri aksayacak olsa bile diğer şubeler arasında havale işlemleri devam edebilecek ve veri kayıtları tüm şubelere dağıtıldığı için gayet güvenli bir altyapı kurulmuş olacaktır.

Tür 4: Bütünüyle İzin Gerektiren Blokzincir Ağları (Özel-Private)

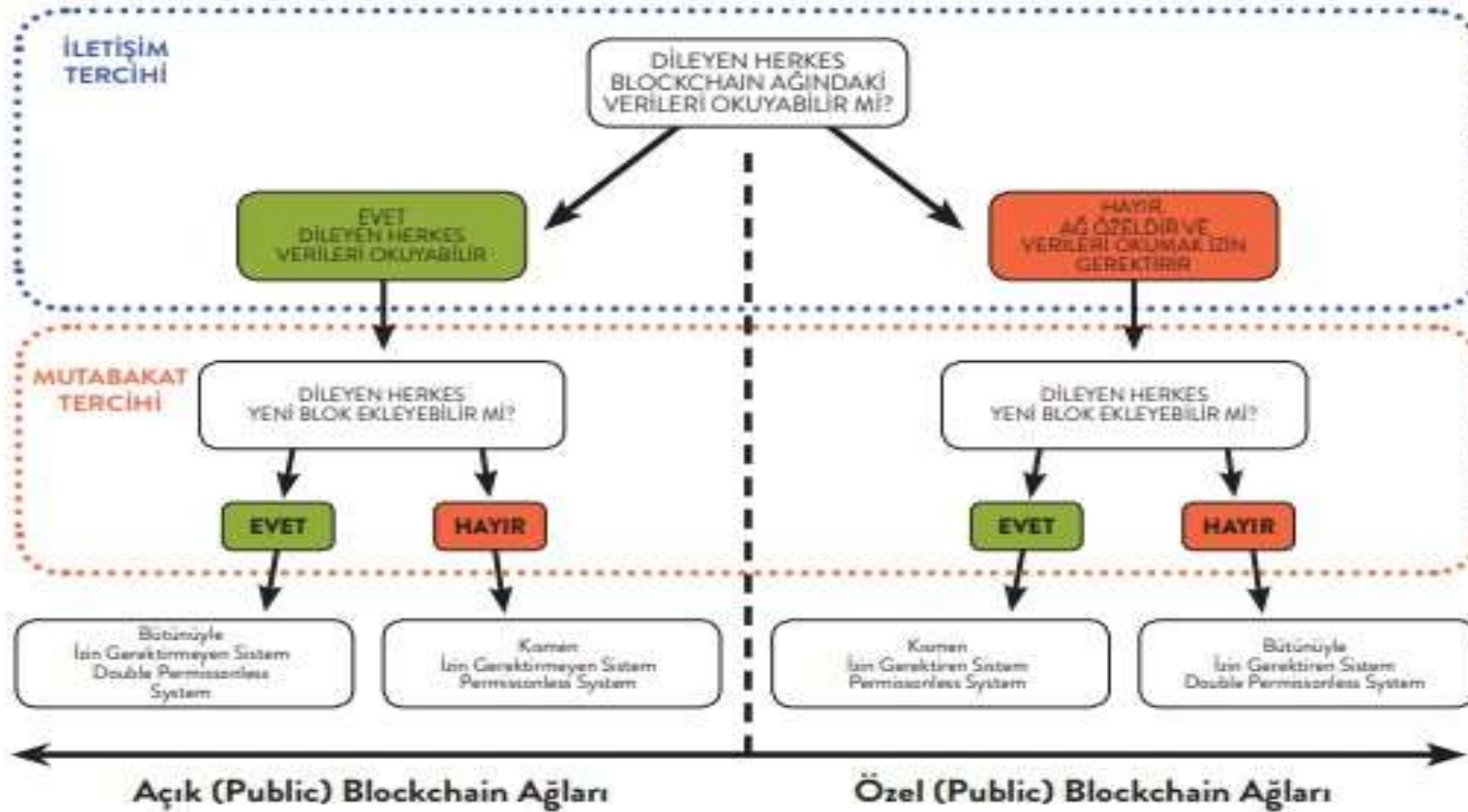
- Eğer bir Blokzincir ağına girerek kayıtlı verileri okumak için izin almamız gerekiyorsa ve sonrasında bu ağın “mutabakat yapısına” uyarak yeni bloklar eklemek ve “mutabakat sürecine” dahil olmak için tekrardan izin gerekiyorsa, bu tarz ağlara ***Bütünüyle İzin Gerektiren Blokzincir Ağları*** adı verilir.

Gerçek hayattan farazi bir örnek olarak bankalar arasındaki EFT işlemleri örnek gösterilebilir. Bir EFT işlemi için tüm bankalar arasında kurulan özel bir Blokzincir ağına girmek gerekmektedir ve içeriye giriş izni için bir banka olmak gerekmektedir. Sisteme giren bankalar içindense sadece kendi aralarında EFT yapacak iki şubeye veri yazma izni verilmektedir. Böylece bu kayıtlar sadece banka ve şube seviyesinde tutulacaktır. Sisteme izin verilen bankaların ve şubelerin hepsi verileri okuyabilir, ancak “mutabakat yapısı” gereği “mutabakat sürecinde” kayıt oluşturma izni sadece kendi arasında işlem yapan iki şubede olacaktır.

Kaynak: Blockchain 101, Ahmet Usta, Serkan Doğantekin

Blokzincir Türleri Özet

Şekil 8: Blockchain Türleri



Blokzincir Teknolojisinden Etkilenecek Konular

Blokzincir teknolojisinin en etkileyici özelliği, web'in kuruluşundan sonra iş yapış şekillerini değiştirecek, hukuki, finansal, toplumsal bu değişimlere sebep olacak «*güven problemini*» ortadan kaldırmasıdır.



Bu güven unsuru özelliği ile işlem yaptığınız tarafı tanıyın - tanımayın, araya bir merkez, aracı, noter, banka, 3. parti vs. dahil etmeden ilerlemek an meselesidir. Bu özellik, *mahremiyet*, *hız ve maliyet* açısından da çok olumludur.

Genel kanı; aracılık hizmeti sunan kurumlar ve yöntemler yakın gelecekte ya *kabuk değiştirecek* ya da zamanla *yok olacaklar..*

?Kim bu Aracılar?



Akıllı Sözleşme (Smart Contract) Örnekleri

Aydın'ın Çine ilçesinde Jeotermal enerji santrali kurulması gündemde olsun.



Negatif durum

- Çevreye zararı,
- Ekolojik dengeyi bozması,
- İklimi olumsuz etkilemesi

Pozitif durum

- Yenilenebilir enerji üretimi,
- Yerel ekonomiye katkısı,
- İstihdamı artırması

Nasıl karar vereceğiz?

Jeotermal'i yapacak şirket 5 yıl boyunca ilçe ve civar köyde 100 kişiye istihdam sağlayacağını ve 500 kişilik ilkokul yaptıracığı sözünü vermiş olsun.

Akıllı sözleşme ile köylülerin kısıtlamaları belirtilir. 5 yıl boyunca istihdam sağlama ve okul inşa etme sözü tutulursa JES üzerindeki kısıtlama kalkar.

Buna rağmen JES onaylanmalı mı? Burada akıllı sözleşmedeki girdiler oylanacak (JES yapılsın / yapılmasın) E/H şeklinde. JES'in yapılacağı ilçede oy kullananların kat sayısı 5 iken, Aydın'da 3, Ege''de 2 ve Türkiye'de 1 sayılsın.

Greenpeace - Bağış Örneği (Akıllı sözleşmeler)

Kuzey kutbunda kaçak balina avlayanlarla mücadeleyi etkin sürdürmek için proje geliştiren Greenpeace'in finansmana ihtiyacı vardır ve bağış talep eder.



Negatif durum

- Yapılacak bağışların gerçekten projeye harcanıp harcanmadığının bilinmemesi

Pozitif durum

- Bağışlarla birlikte balinaların hayatına devam etmesinin sağlanması

Greenpeace STK ile
bağışçılar arasında bir
akıllı kontrat
tasarlansın.

1) Proje için faaliyette
bulunacak Gemi 2
yıllığına kiralandığında
Bağış havuzundan 5
milyon \$,

2) Mürettebat
kadrosuna 4 doktoralı,
2 masterlı dahil
edildiğinde 1 milyon \$,

3) Gemi limandan
çıktığında 500 bin \$,

4) Gemi aralıksız 60
günü kuzey kutbunda
tamamladığında 3
milyon \$ Greenpeace'e
aktarılacaktır.

4.Bölüm

Blokzincir Uygulamaları ve Diğer Kripto Paralar

Para ve Jeton Farkı (Coin vs Token)

ICO ve Venture Capital (Risk Sermayesi)

Cüzdan Türleri

Sıcak Cüzdanlar

Soğuk Cüzdanlar

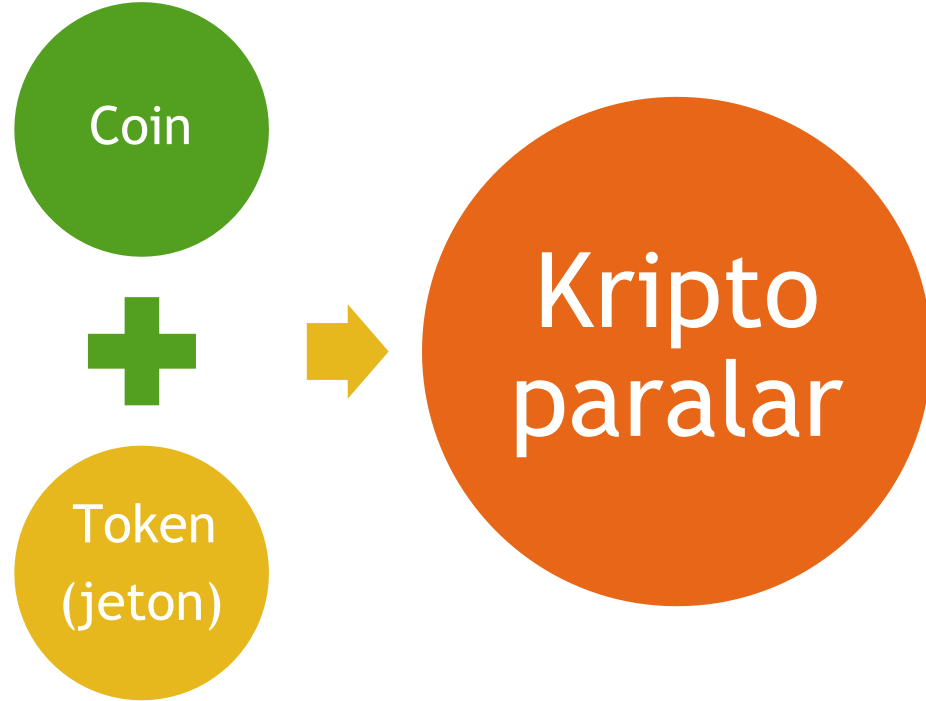
Bitcoin ve Ethereum Arasındaki Farklar

Bazı Altcoin'lerden Örnekler

Dersin Sorumlusu: Öğr. Gör. Olcay YILMAZ

Kaynak: Vedat Güven, Erkin Şahinöz. Blokzincir, Kripto Paralar, Bitcoin, 2018.

Para ve Jeton Farkı (Coin vs Token)



ICO (Başlangıç - İlk Coin Arzı)



Venture Capital (Risk - Giriřim Sermayesi)



Fikrin var, projen var.
Fona gereksinimin
var. Bankalar krediye
yanařmıyor.

Risk giriřim sermayeleri
projene fon saęlarken,
*aynı zamanda řirketine
ortak oluyor.*

Elektronik Cüzdanlar



Kripto varlıklarımızı
sakladığımız yazılım,
uygulamadır.



Blokzincir üzerinde
para göndermek,
almak, bakiyeyi
kontrol etmek
amacıyla kullanılan,
açık ve gizli anahtar
çiftini üreten,
saklayan yazılımdır.

Gizli - Özel anahtarın önemi

- ▶ Doğrulama, teyit etme yahut hesaba erişme noktasında başvurulana, kimseyle paylaşmamamız gereken anahtar (bir nevi kod, şifre)
- ▶ Özel anahtarın kaybı, unutulması durumu..
- ▶ Sistem eksik mi kötü mü? (Geleneksel de nasıl) şifreni unutsan, çaldırsan?

Kritik Soru

- Özel anahtar kaybedilmedi, para çalınmadı.. Unuttunuz sadece şifrenizi.. Hatırlamıyorsunuz..

Aracı kurum ile kendini kanıtladığında, yeni şifre temin etmek mümkün. Müşteri temsilcisi var.

Şahsına Kripto Cüzdanında oluşturulan Gizli anahtarın kaybedilmesi durumunda muhatap yok. Soğuk su içebiliriz.

Kritik Soru

- Merkezi Kripto para borsalarından (paribu, btctürk, binance vs.) kripto para aldık. Varlıklarımızı burada tutsak.. Şahsımıza özel cüzdan yerine..



Cüzdan Türleri



- *Online Cüzdanlar*
- *Masaüstü cüzdanlar*
- *Mobil cüzdanlar*



- *Kağıt Cüzdanlar*
 - *Beyin*
 - *Donanım cüzdanlar*

<https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html>

<https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html>

- 1) <https://beincrypto.com.tr/ogren/2020nin-en-iyi-15-bitcoin-cuzdani/>
- 2) <https://www.bitcoingundem.com/2020-yili-en-iyi-sicak-ve-soguk-bitcoin-cuzdanlari-neler/>
- 3) <https://www.bfmedia.io/haberler/2020-yilinda-kullanabileceginiz-en-iyi-20-kripto-cuzdani-9229.html>
- 4) <https://www.kaspersky.com.tr/blog/cryptowallets/4838/>

Ethereum ve Bitcoin Arasındaki Farklar



Blokların içerisindeki datalar akıllı kontratlardan oluşur.



Ethereum'da ise taraflar sözleşme veya anlaşma şartlarını koda, programlamaya dökerek hareket eder. (se,sa)



ETH işlemlerinde teyit ilkesi gereği mutabakat POS ile sağlanmaktadır.

Ethereum'un arzı sınırlı değildir. Blok üretimi için hash değerini en hızlı bulan madenciye 5 ether ödül verilirken, sözleşmelere komut girmek, not yazmak, değişiklik yapmak istenildiğinde de «ether» ödenmektedir.



Blokların içerisindeki datalar para transferindeki sahiplik değişimlerinden oluşur.



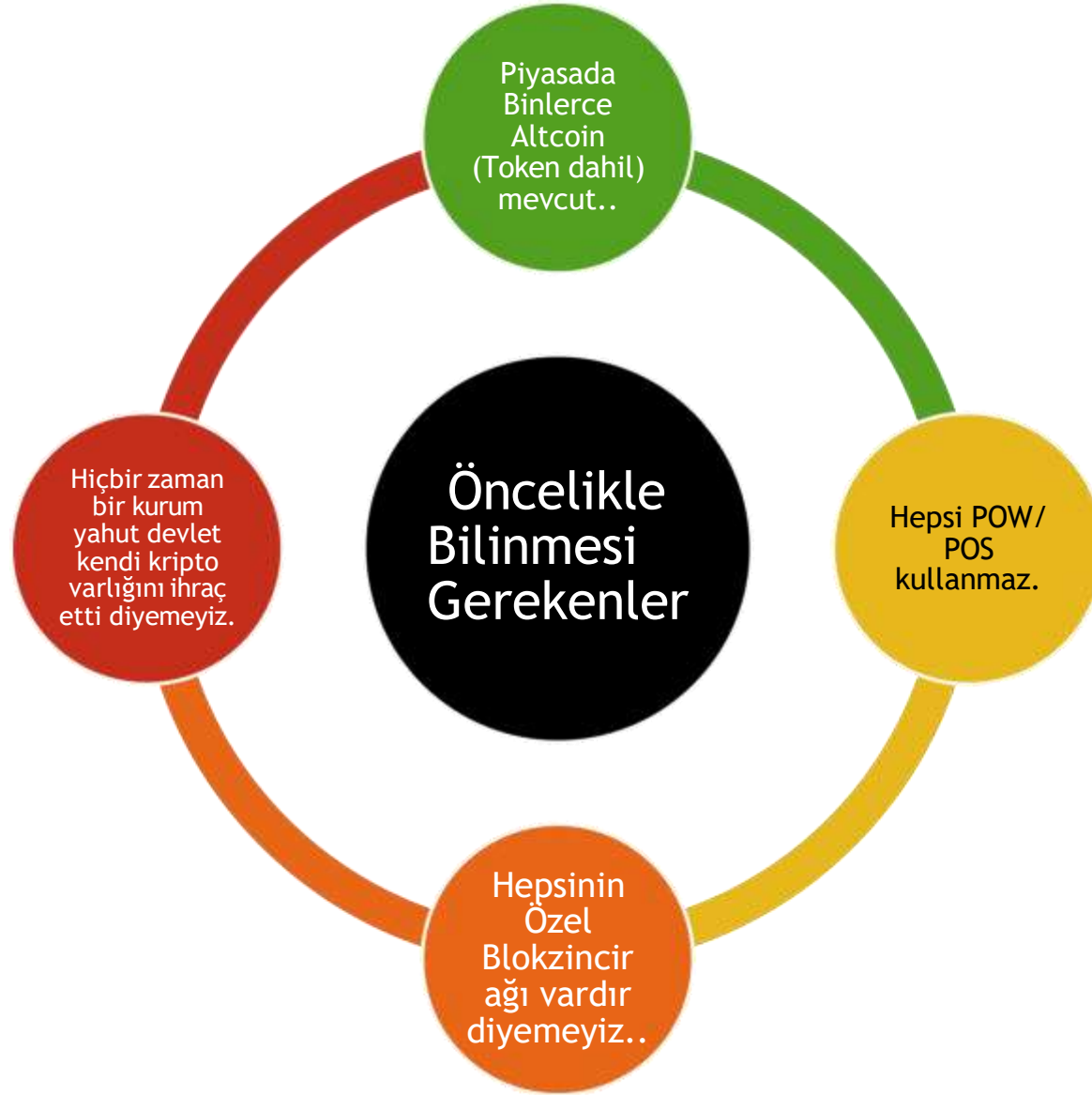
Bitcoin' de taraflar arasında sadece bir değer-sahiplik transferi var. (BTC sadece para gibi kullanılabilir).



BTC işlemlerinde teyit ilkesi gereği mutabakat POW ile sağlanmaktadır.

BTC'nin ise arzı 21 milyon ile sınırlıdır. Blok üretimi için hash değerini en hızlı bulan madenciye an itibariyle 6,25 BTC ödül verilirken, bu tutar her 4 yılda bir yarılanmaktadır. Nedeni BTC'nin arzının sınırlı olması ve günden güne sona yaklaşmasındandır.

Bazı Diğer Altcoinler



Tüm Kripto Paraların Ortak Özellikleri

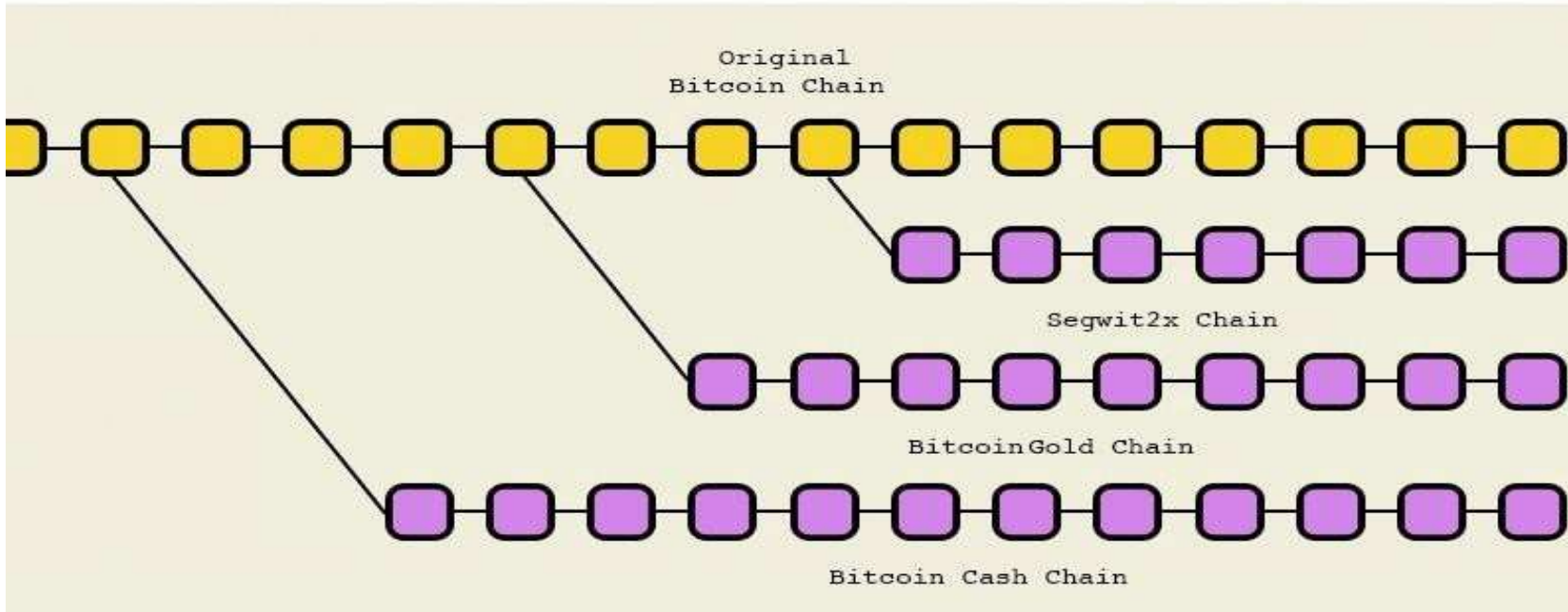


Bitcoin Cash - BCH

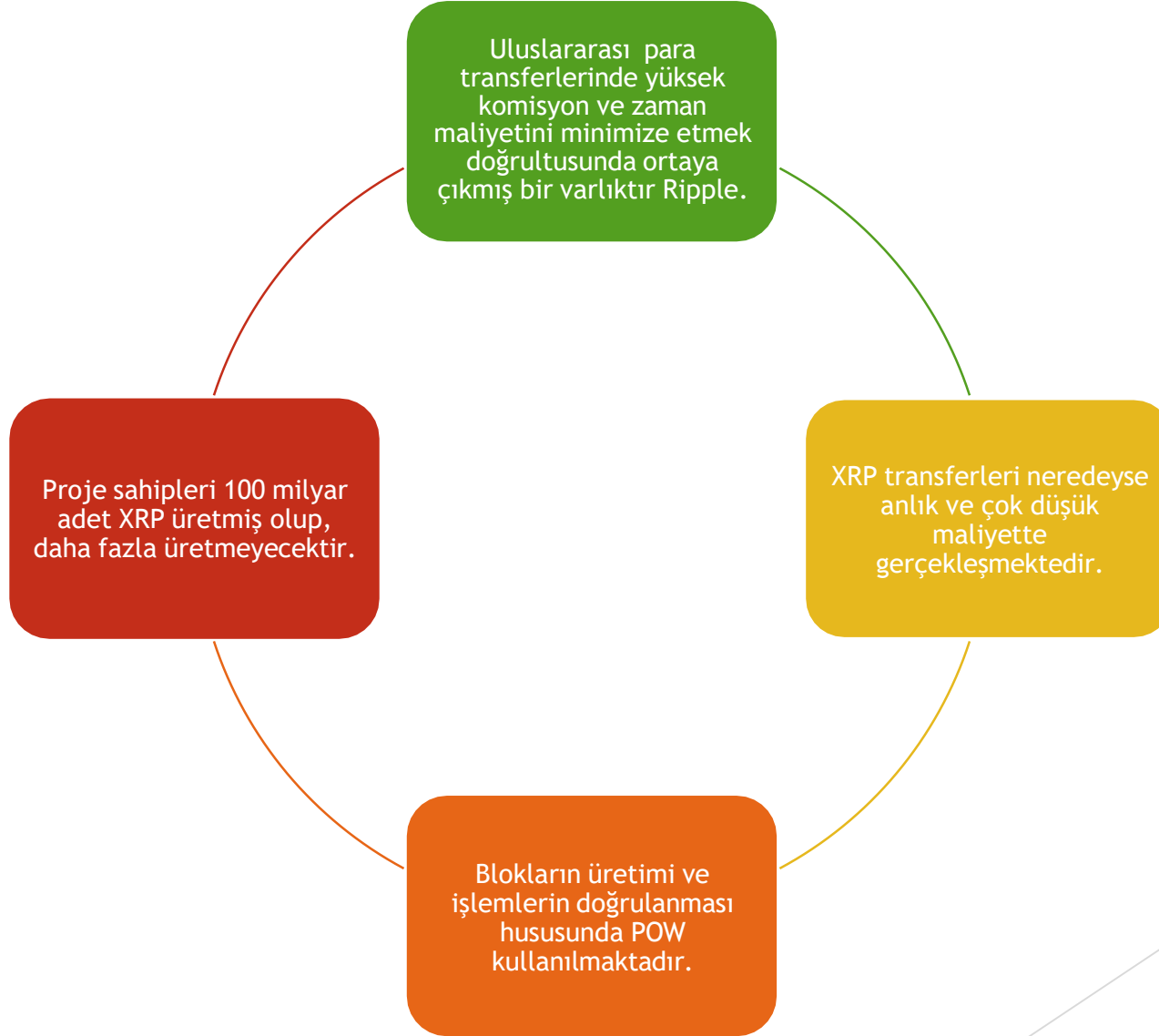


1 Ağustos 2017'de mecburi çatallanma ile hayatımıza giren bir alt coindir. Ana zincirden ayrılması ile Blok boyutu limiti 1 MB değil 8 MB'dir.

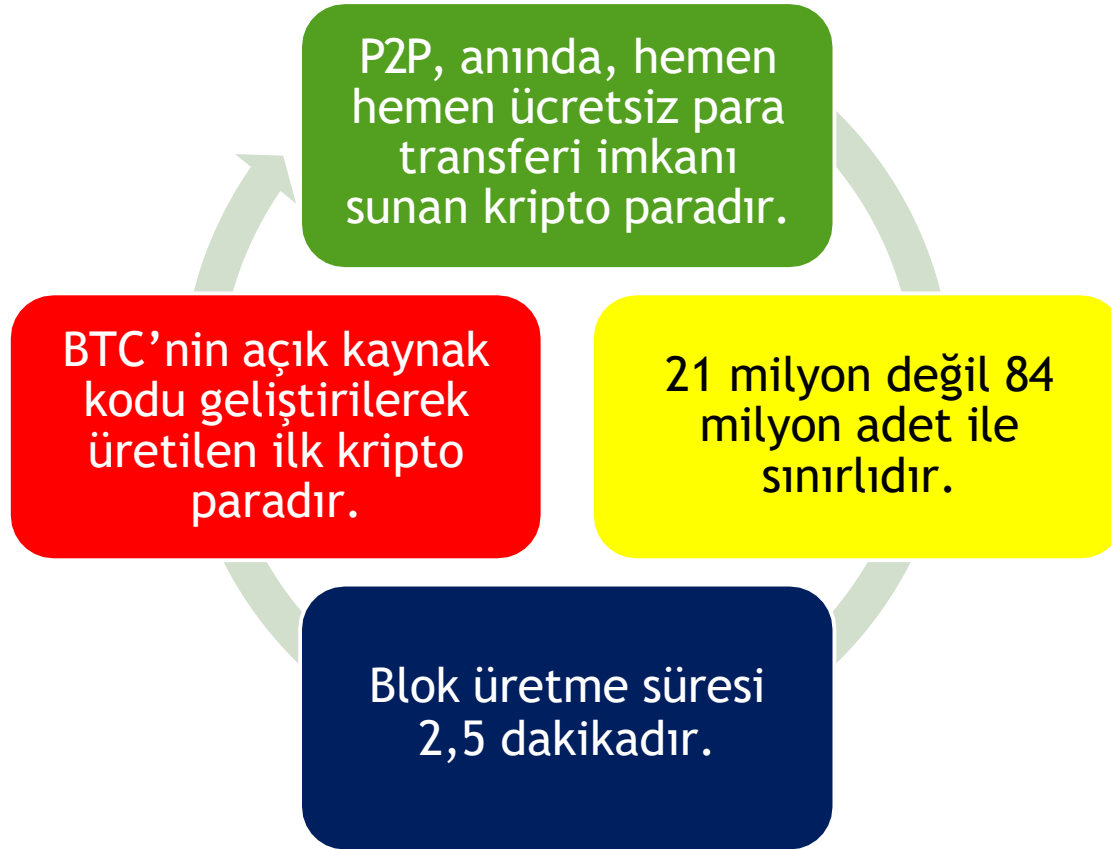
BITCOIN FORK ATTEMPTS



Ripple -XRP



Litecoin - LTC



Monero - XMR



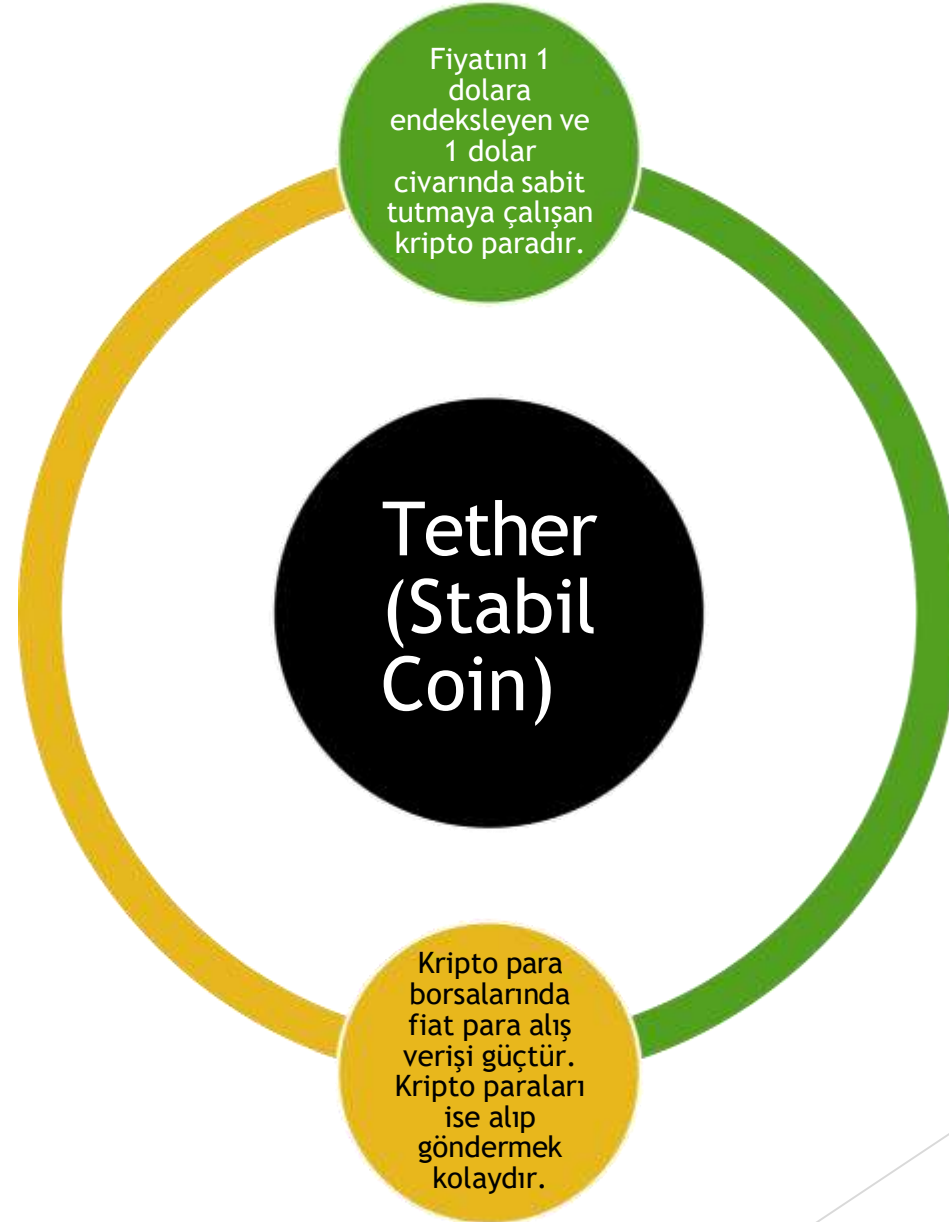
Açık kaynak kodlu, merkezi olmayan yapıda, işlemlerin bloklara kaydedildiği, madencilik yapılarak yeni üretimlerin gerçekleştiği kripto paradır.



Monero'da birkaç göndericinin gönderme işlemleri gruplanır ve tek mesaj olarak gönderilir. Parayı gönderenin rassal datası ile alacak olanın açık anahtarı kullanılır ve bu transfere özel anahtar çifti üretilir.



BTC'den tek ve en büyük farkı tam gizliliği ve takip edilememesidir.



Cardano - ADA



Japonya kökenli olup, POS algoritmasını kullanan akıllı sözleşme platformudur.



Bankacılık ürün ve hizmetlerinin pahalı olduğu ve özellikle gelişmekte olan ülkelerde Blokzincir tabanlı projelerle finansal hizmetler sunmaktadırlar.

Tron - TRX



*Ürün geçmişini takip etme
amacıyla geliştirilen bir
projedir.*

*Her türlü ürün ve hizmet ile
ilgili bilgilerin zaman damgalı
kaydedilmesi,
değiştirilememesi ve takip
edilmesi imkanını Blokzincir
tabanlı sunar.*

Dogecoin - DOGE



Şaka parası olarak bilinirken, Bitcoin kodlarını kullanan, blok üretim süresi 1 dakika olup arzı sınırsızdır.

Ekosisteme katkısı:
Çok yüksek üretimi sonucu fiyatı düşük çıkmıştır. Ucuz olduğu için insanlar 3-5 bin para transferi yapmaya başlamışlardır.

Ekosisteme katkısı:
1) Kripto para transferlerinin öğrenilmesi, yaygınlaşmasını sağlamıştır.
2) İnternet ortamında like ve alkış yerine kaliteli içeriklere bahşiş alışkanlığı yerleşmiştir.

Bahşiş süreci bahşiş ekosistemini de filizlendirmiştir. 2014 SOÇİ olimpiyatları için Jamaika kızak takımına yardım kampanyasında 36K dolarlık dogecoin bahşiş toplanmıştır.

SON