

# Blokzincir Üzerine

Halil Kemal Taşkın

# **İçerik**

**Özet fonksiyonlar**

**Blokzincir**

**Kripto para'nın hikayesi**

**Fikir birliği algoritmaları**

**Havuz problemleri**

**Blokzincir uygulamaları**

**Alternatif Madencilik**

**Blokzincir alternatifleri**

# Bu Sunumda Neler Yok?

- Yatırım tavsiyesi
- Hangi coin ne kadar eder?
- Nasıl alıp satıyoruz?
- Neyi nereden alırız?

# Blokzincir hacker'ı olmak

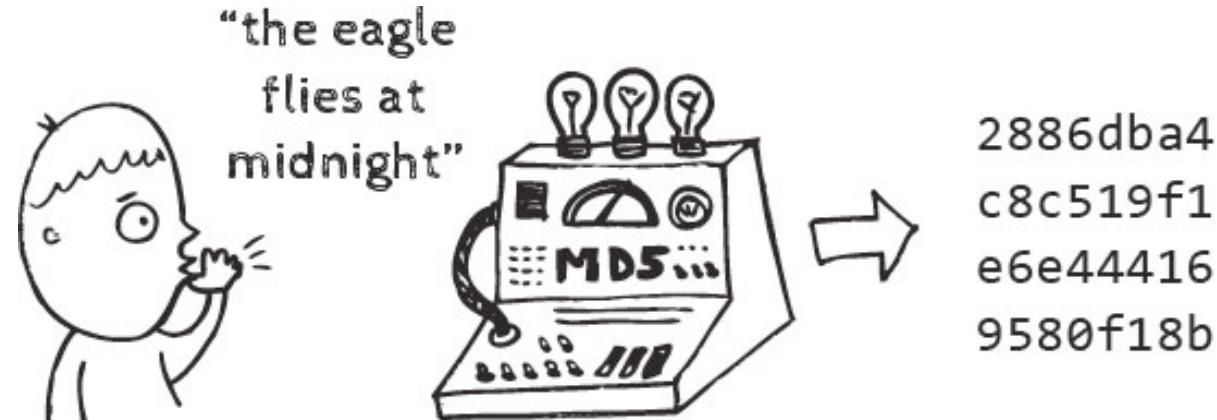
- ?

# Özet fonksiyon

- Criptografi'nin temel yapı taşlarından birisidir.
- Her boyuttan bilgiyi sabit uzunluklu bit dizisine dönüştüren fonksiyonlara denir.

Bu dönüşüm öyle olmalıdır ki verideki en ufak bir değişiklik özet değerini değiştirmelidir.

- Tek yönlü (one-way) fonksiyonlar olarak da adlandırılırlar.
- Teorik olarak tek yönlü olması mümkün değildir. Ancak pratikte öyle olduğu varsayıılır.



# Kriptografik Özет fonksiyon

İdeal bir kriptografik özet fonksiyonu şu dört özelliği sağlamalıdır:

- Herhangi bir mesaj için özet hesaplamak kolay olmalıdır.
- Özeti değiştmeyecek şekilde mesajı değiştirmek zor olmalıdır.
- Aynı özete sahip iki farklı mesaj bulmak zor olmalıdır.
- Bilinen bir özet değerini verecek mesajı bulmanın tek yolu her mesajı denemek olmalıdır.
- Popüler Algoritmalar: ~~MD5, SHA1~~, SHA256, SHA3

# $2^{128}$ ne kadar büyük olabilir ki?

- Evrenin yaşı:  $\sim 14$  milyar yıl  $\sim 2^{58}$  saniye
- Evrendeki yıldızların sayısı  $\sim 2^{80}$
- Evrendeki tüm atomların sayısı  $\sim 2^{265}$
- Örnekler:
- 16'lık (Hexadecimal) Gösterim:  
**b2b31a1c59f53e58b2466f3be660a212**
- 2'li (Binary) Gösterim:

```
001100010011001000110011001101000011010100110110001101110011100  
0011100100110000010000010100001001000011010001000100010101000110
```

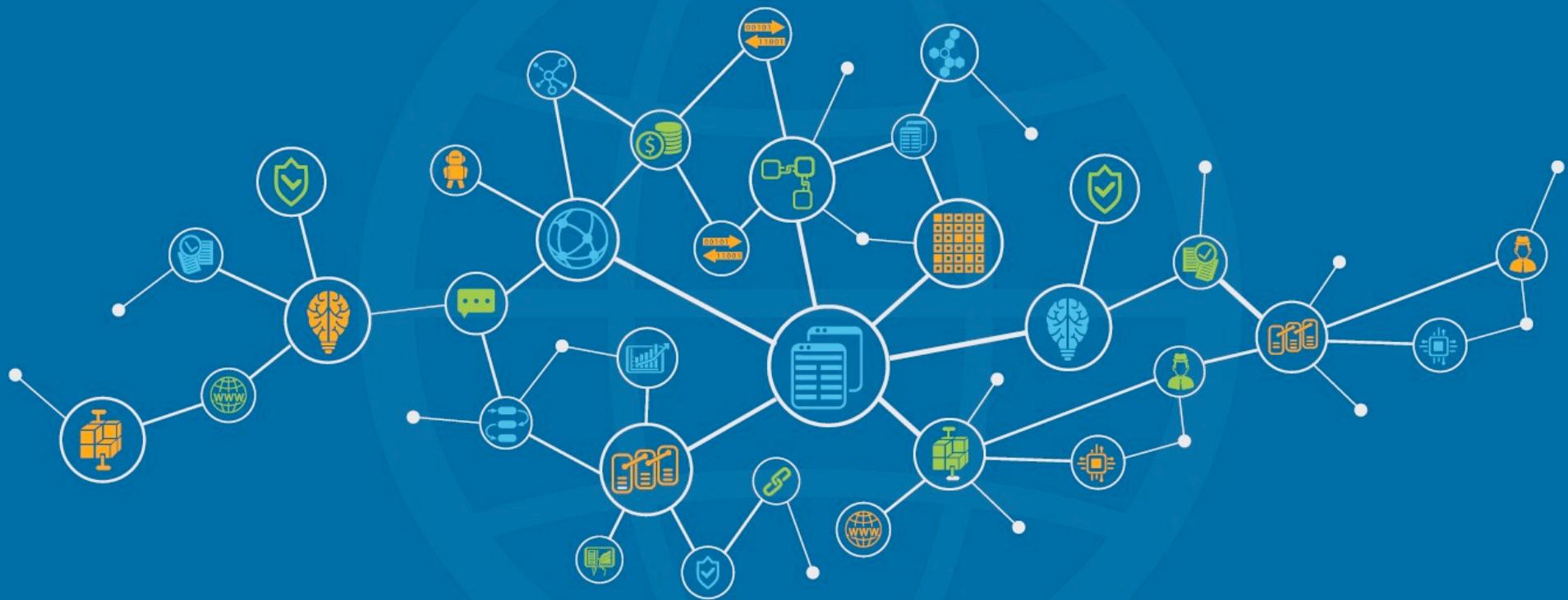
# $2^{128}$ ne kadar büyük olabilir ki?

- 128-bit anahtar için tüm uzayı aramak isteyelim.
- Her çekirdek saniyede  $2^{48}$  deneme yapın. ( $\approx 300\text{ THz}$  işlem gücü)
- Dünyadaki insan sayısı: 7 Milyar  $\approx 2^{33}$
- Her insan  $1024 (= 2^{10})$  çekirdekli bilgisayara sahip olsun.

$$\frac{2^{128}}{\approx 2^{33} \cdot 2^{10} \cdot 2^{48}}$$

- Toplam Süre  $\approx 2^{37}$  saniye.
- $\approx 1.6$  Milyon gün.

# Blokzincir'in hikayesi



# İlk Mesajlar

From: "Satoshi Nakamoto" [satoshi@anonymousspeech.com](mailto:satoshi@anonymousspeech.com)

Sent: Friday, **August 22, 2008** 4:38 PM

To: "Wei Dai" <[weidai@ibiblio.org](mailto:weidai@ibiblio.org)>

Cc: "Satoshi Nakamoto" [satoshi@anonymousspeech.com](mailto:satoshi@anonymousspeech.com)

Subject: Citation of your b-money page

I was very interested to read your b-money page. I'm getting ready to release a paper that expands on your ideas into a complete working system. Adam Back ([hashcash.org](http://hashcash.org)) noticed the similarities and pointed me to your site.

I need to find out the year of publication of your b-money page for the citation in my paper. It'll look like:

[1] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, (2006?).

# İlk Mesajlar

From: Satoshi Nakamoto

Sent: Saturday, **January 10, 2009** 11:17 AM

To: weidai@weidai.com

Subject: Re: Citation of your b-money page

I wanted to let you know, I just released the full implementation of the paper I sent you a few months ago, Bitcoin v0.1. Details, download and screenshots are at [www.bitcoin.org](http://www.bitcoin.org)

I think it achieves nearly all the goals you set out to solve in your b-money paper.

The system is entirely decentralized, without any server or trusted parties. The network infrastructure can support a full range of escrow transactions and contracts, but for now the focus is on the basics of money and transactions.

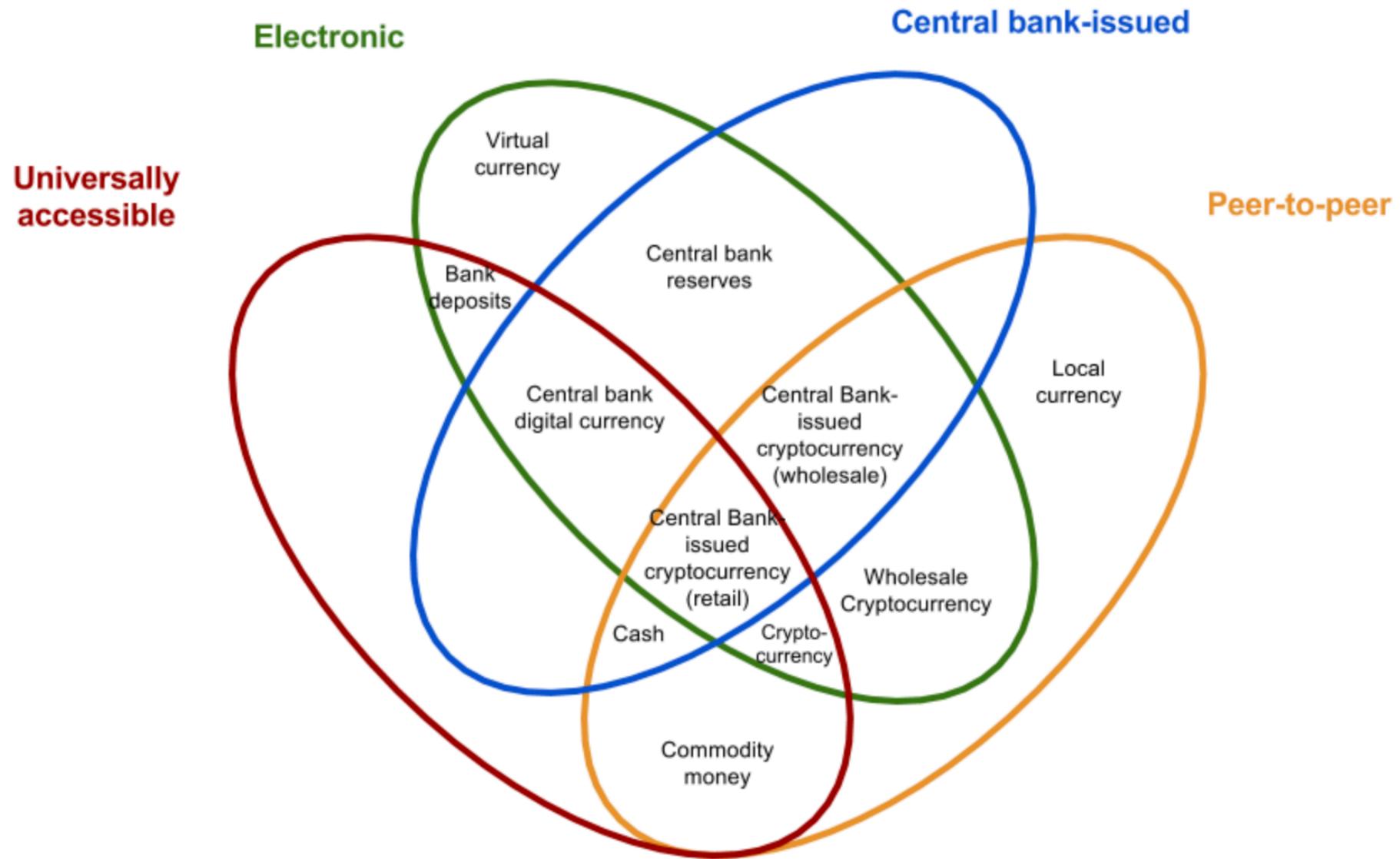
# İlk Mesajlar

A screenshot of a web browser window displaying a forum post from the P2P Foundation. The browser's address bar shows the URL: p2pfoundation.ning.com/forum/topics/bitcoin-open-source. The page header features the P2P foundation logo and the text "The Foundation for Peer to Peer Alternatives". Below the header, a navigation menu includes links for Main, My Page, Members, Videos, Forum (which is highlighted in blue), Groups, Blogs, and Chat. Under the Forum link, there are two options: All Discussions and My Discussions, with a "+ Add" button to the right. The main content area displays a post by Satoshi Nakamoto titled "Bitcoin open source implementation of P2P currency", posted on February 11, 2009, at 22:27. The post text reads: "I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper: Download Bitcoin v0.1 at <http://www.bitcoin.org>". A note below states: "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."

# Satoshi Nakamoto

- Satoshi Nakamoto isimli birisi 2009 tarihinde bir e-posta ile sistemi Bitcoin isimli “kripto para” sistemini tanıttı.
- Bazı forumlarda da paylaştı.
- İlk başlarda sadece kendisi madencilik yaptı.
- Daha sonra birkaç kişi daha katıldı.
- Hesabında ~1M BTC var.
- 2011 den beri herhangi bir haber alınamıyor.

# Kripto para != Elektronik para



<https://bitcoin.org/bitcoin.pdf>

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model

# Blokzincir'in tasarım Özellikleri

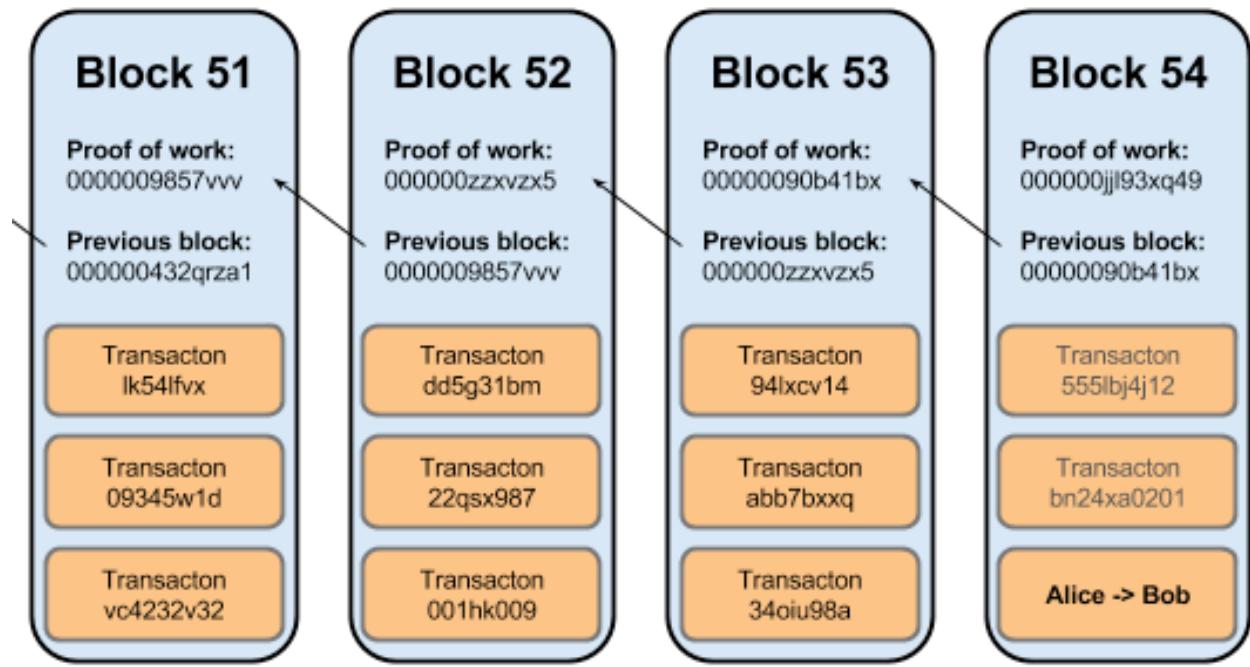
- Tüm kayıtların tutulduğu, açık ve değiştirilmeye dayanıklı bir defter.
- Güvenilir üçüncü tarafa ihtiyaç yok [!]
- Çoğunluğun dürüst olduğu varsayıımı üzerine kuruludur. (>%51)
- P2P ağlar üzerinde dağıtık olarak çalışmaya uygun
- Pseudonymity'yi sağlar.
- Anonimlik (Anonymity) sağlamaz [!]

# Blokzincir Bileşenleri

- Blok
- Dağıtık iletişim altyapısı
- Fikir birliği algoritması ve protokolü (Consensus Algorithm)
- Madenciler
- Fikir birliğini sağlamak için gerekli gönüllü uçbirimler (“node”).
- Kullanıcılar (Her kullanıcı isterse gönüllü uçbirim de olabilir.)

# Blokta Neler Var?

- Önceki bloğa ait PoW özet değeri
- Zaman damgası
- PoW değeri
- Veri (transfer işlem listesi vb.)
- “Nonce” değeri



# Fikir Birliği Algoritmaları (Consensus Algorithms)

- **PoW** : Proof-of-Work
- **PoS**: Proof-of-Stake
- **PoA**: Proof-of-Authority
- **PoC**: Proof-of-Capacity

# PoW: Proof-of-Work

- Algoritma: İlk n-bit değeri 0 olan sayıdan daha küçük sayı bul!
- Birşeyi kazanmak için emek harcadığınızı ispatlamak.

**Popüler Örnekleri:** Bitcoin, Ethereum, Litecoin, Dogecoin

**Artılar:** Kesin olarak sonuç veriyor, sorunsuz çalışıyor.

**Eksiler:** Dünyayı tüketiyor.



# Hashcash

Adam Back tarafından 1997 yılında önerilmiştir.

The screenshot shows the homepage of hashcash.org. The left sidebar contains links for home, faq, documentation, mailing-list, news, media articles, bitcoin, mail plugins, blog plugins, binaries, source, benchmarks, biggest stamp, developers, java applet, and papers. Below the sidebar are icons for web, hashcash.org, and Google Search, along with a hits counter for November 03. The main content area features a large heading "Hashcash". It describes Hashcash as a proof-of-work algorithm used for denial-of-service countermeasures. It explains that a hashcash stamp requires work to compute and can be verified efficiently by anyone. It notes its use in Bitcoin mining and email anti-spam. The source code is simple and can be verified by eye. A bulleted list at the bottom provides links to FAQ, format info, the original paper, and the new domain. The footer contains a note about Microsoft's incompatible spec and a link to the original paper.

hashcash.org

[home](#)  
[faq](#)  
[documentation](#)  
[mailing-list](#)  
[news](#)  
[media articles](#)  
[bitcoin](#)  
[mail plugins](#) ▾  
[blog plugins](#) ▾  
[binaries](#) ▾  
[source](#) ▾  
[benchmarks](#)  
[biggest stamp](#)  
[developers](#)  
[java applet](#)  
[papers](#)

web hashcash.org  
Google Search

hits since nov 03

[Hashcash FAQ](#).  
[Hashcash format info](#).  
[Hashcash Paper Aug 02 - "Hashcash - A Denial of Service Counter-Measure"](#) (5 years on), Tech Report, Adam Back  
The site is slowly moving over to this new domain, some of the content is still here: <http://www.cypherspace.org/hashcash/>

If you have questions or are interested to port to different systems, integrate into different email clients (MUAs), anti-spam systems, or MTAs email [Adam Back adam@cypherspace.org](mailto:Adam_Back_adam@cypherspace.org) or post on the [hashcash-list](#).

Microsoft released an incompatible hashcash spec [email postmark](#) which I believe is implemented in exchange, outlook, hotmail etc microsoft mail related infrastructure as part of their coordinated spam reduction initiative [CSRI](#). They hash the body rather than the recipient, and they also use a modified SHA1 as the hash, and use multiple sub-puzzles to reduce variance.

# Bitcoin



- Merkezi bir otorite olmadan finansal işlemleri gerçekleştirmeyi sağlar.
- Tüm kayıtların tutulduğu tek bir açık defter vardır.
- Fikir birliği için PoW yöntemini kullanır.
- Dağıtık bir yapı (P2P) kullanarak açık defter saklanır.

# Bitcoin Protokolü ve Kuralları

- Kripto para birimi BTC'dir.
- 1 Satoshi= 0.00000001 BTC
- Her 10 dakikada bir yeni blok üretilip zincire eklenir.
- Zincire yeni bloğun kabul edilmesi için PoW algoritması ile üretilen özet değerinin, gönüllü doğrulama yapan uçbirimlerden en az %51'inin onayı gereklidir.
- Her 2016 blok bulunduktan sonra “zorluk” seviyesi güncellenir.
- Her yeni bloğu bulan madenciye “coinbase” adı verilen ödül BTC verilir.
- Coinbase ile kazanılan BTC, 100 blok sonra kullanılabilir.
- Bir blok içindeki BTC transferi 6 blok sonra kullanılabilir.

# Bitcoin Protokolü ve Kuralları

- Bitcoin transferleri için madenciler komisyon alırlar.
- Coinbase değeri 50 BTC olarak başlamıştır. Her 210.000 blok bulunduktan sonra bu değer ikiye bölünmektedir. Şu anda 12.5 BTC'dir. (~522000. blok üretildi.)
- Bu hesaplara göre;
  - Toplamda en fazla 21.000.000 BTC üretilebilecek.
  - 2140 yılında son Bitcoin üretilicek.
- Blok boyutu en fazla 1MB olabilir.
- Bir blok içine ~2000 işlem sığdırılabilirmektedir.
- Her bitcoin adresi açık anahtarlı kriptografi kullanılarak oluşturulan özel-açık anahtar çifti ile oluşturulur. Özel anahtar sadece kullanıcı da olur. Açık anahtarın “encode” edilmiş hali Bitcoin adresi olarak kullanılır.

# Bitcoin Protokolü ve Kuralları

Bitcoin ağına bağlananlar:

- Tam uçbirimler (Full nodes) (örnek: “Bitcoin Core”)
  - Yeni üretilen bloklar için Bitcoin fikir birliği protokolünü uygulayarak kontrolleri yaparlar.
  - Tam uçbirimler 1. bloktan itibaren tüm blokları saklamak zorundadır.
  - Madenciler: Yeni blok üretmek için ağa bağlanırlar.
- Hafifsiklet Uçbirimler (Lightweight Nodes)
  - Diğer adı: Basit Ödeme Doğrulama İstemcisi (Simplified payment verification (SPV) client)
  - Kullanıcılar tam ya da hafifsikler olarak bağlanabilirler.
  - Pseudonymity'yi sağlar. Anonimlik sağlamaz [!]

**Sistemin güvenilirliği Tam uçbirimlerin sayısı arttıkça artar.**



# BitcoinCore

## Helping you keep Bitcoin decentralized

---

[Download Bitcoin Core](#)

---

Bitcoin Core is programmed to decide which block chain contains valid transactions. The users of Bitcoin Core only accept transactions for that block chain, making it the Bitcoin block chain that everyone else wants to use

It is these users who **keep Bitcoin decentralized**. They individually run their own Bitcoin Core full nodes, and each of those full nodes separately follows the exact same rules to decide which block chain is valid.

There's no voting or other corruptible process involved: there's just individual software following identical rules—"math"—to evaluate identical blocks and coming to identical conclusions about which block chain is valid.

This shared agreement (called consensus) allows people like you to only accept valid bitcoins, **enforcing Bitcoin's rules** against even the most powerful miners.

In addition to improving Bitcoin's decentralization, Bitcoin Core users get **better security** for their bitcoins, **privacy features** not available in other wallets, a choice of **user interfaces** and several other powerful features.

# PoW Tasarım İlkeleri

- Tek bir madde hariç Criptografik Özeti Fonksiyon tasarımları ilkeleri geçerlidir.
- Üretim yapılması istenen ortama göre çeşitleri mevcuttur:
  - CPU etkin tasarımlar
    - Verium, Aeon
  - GPU etkin tasarımlar
    - Ethereum, Zcash
  - ASIC etkin tasarımlar
    - Scrypt ve SHA256 tabanlı kripto paralar
    - Bitcoin, Litecoin

# ASIC Farm



# GPU Farm



# Scrypt: GPU vs. ASIC

## GPU RIG

I made this "cheap" R9 based config:

- **Motherboard:** ASRock H81 Pro BTC (PCI-E x5): 54.95 €
- **CPU:** Intel Celeron G1840 : 44.75€
- **RAM:** Crucial Ballistix Sport 4Go DDR3 : 25.35€
- **GPU:** 3x AMD Radeon Sapphire R9 290 Tri-X (Used) : ~600€
- **SSD:** Corsair Force Series LS 60 Go : 41.95€
- **Power Supply:** Be Quiet ! Power Zone 1000W 80PLUS Bronze : 184.95€

**Total:** 951.95 € = 1 095.62 \$

**Litecoin average hashrate:**  $3 \times 800 \text{ kH/s} = \sim 2.4 \text{ MH/s}$  = 16.41 LTC / Year = 0.13 BTC / Year

**Monero average hashrate:**  $3 \times 700 \text{ H/s} = \sim 2.1 \text{ kH/s}$  = 561.15 XMR / Year = 1.209 BTC / Year

**Power consumption:** ~1kWh => ~ 130€ / Year

## Scrypt ASIC

From the same range of price, I found the Zeusminer LIGHTNING X6 + 1200W PSU (both used)

**Total:** 1 100 € = 1 238.21 \$

**Litecoin average hashrate:** ~ 42 MH/s = 287.17 LTC / Year = 2.29 BTC / Year

**Power consumption:** ~1kWh => ~ 130€ / Year

# Scrypt is Maximally Memory-Hard

Joël Alwen<sup>1</sup>, Binyi Chen<sup>2</sup>, Krzysztof Pietrzak<sup>1</sup>, Leonid Reyzin<sup>3</sup>, and  
Stefano Tessaro<sup>2</sup>

<sup>1</sup> IST Austria

{jalwen,pietrzak}@ist.ac.at

<sup>2</sup> UC Santa Barbara

{binyichen,tessaro}@cs.ucsb.edu

<sup>3</sup> Boston University

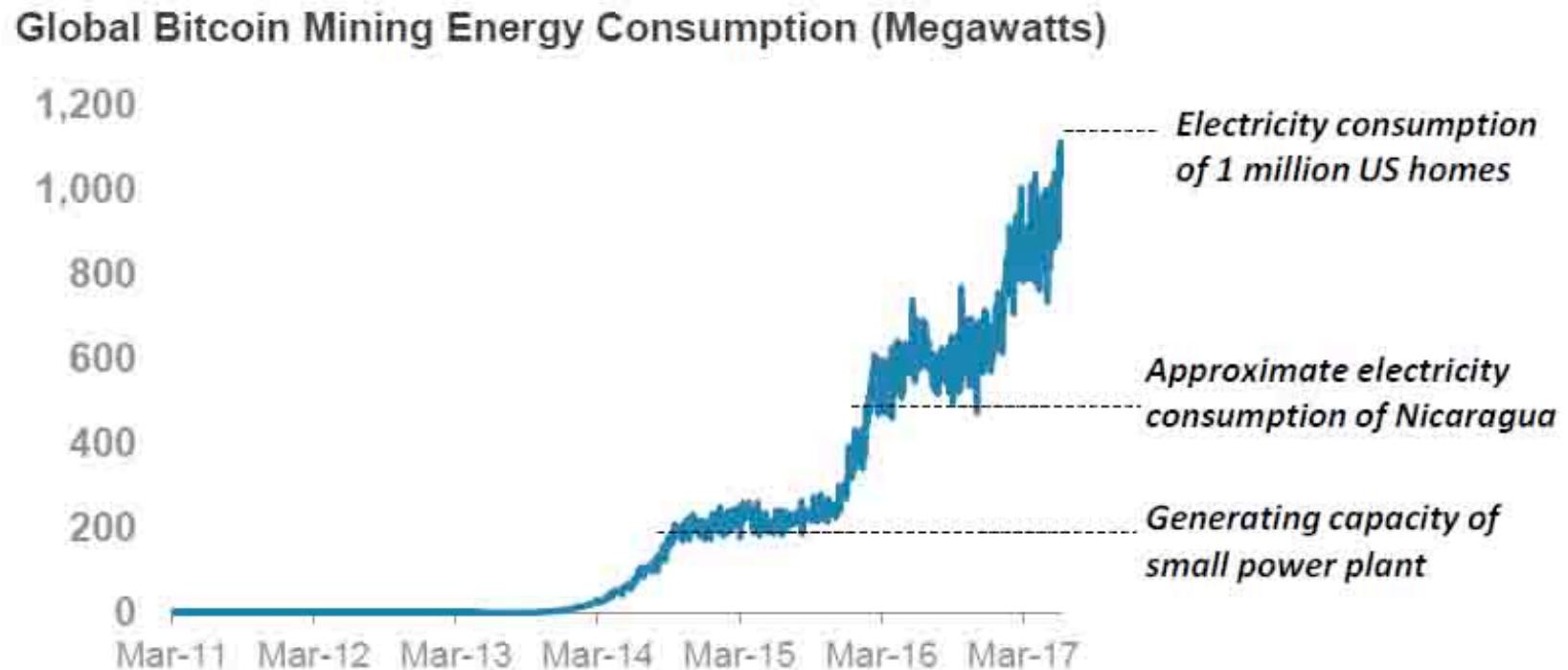
reyzin@cs.bu.edu

**Abstract.** Memory-hard functions (MHFs) are hash algorithms whose evaluation cost is dominated by memory cost. As memory, unlike computation, costs about the same across different platforms, MHFs cannot be evaluated at significantly lower cost on dedicated hardware like ASICs. MHFs have found widespread applications including password hashing, key derivation, and proofs-of-work.

- <https://eprint.iacr.org/2016/989>
- <https://www.youtube.com/watch?v=ot0eoYTgE48>

# Enerji Tüketimi

- Madencilik için harcanan enerji bazı ülkelerden fazladır.
- Madencilik için kullanılan cihazların verimliliği artmasına rağmen toplam enerji tüketimi artmaktadır.
- Tüketilen enerjinin %80'den fazlası çöpe gitmektedir. [!]



# Madencilik Havuzları

# pooled mining

/pu:lđ 'mʌɪnɪŋ/

*combines the work of many  
miners toward a common goal*



# Madencilik Havuzları

- Birlikten güç doğar.
- Büyük havuzlar Çin merkezli.
- Havuza dahil olanlar işlem güçlerini paylaşırlar.
- Tek bir bloğun bulunması için gerekli olan PoW algoritması sonucu için olan denemeler paylaşılır.
- Komisyon alarak çalışırlar. Yeni blok bulunması sonucu elde edilen gelir, işlem gücü paylaşım oranına göre dağıtılır.

**Bitcoin için harcanan işlem gücünün yaklaşık %80'i boş gitmektedir.**

Pool	Blocks	%
unknown	187,781	35.93%
DiscusFish / F2Pool	40,610	7.77%
AntPool	35,610	6.81%
BTC Guild	32,951	6.31%
DeepBit	31,105	5.95%
Slush	23,921	4.58%
GHash.IO	23,101	4.42%
Bitfury	17,881	3.42%
BTCC	17,728	3.39%
BW Pool	12,328	2.36%
Eligius	11,436	2.19%
BTC.com	10,683	2.04%
ViaBTC	8,517	1.63%
BTC.TOP	8,250	1.58%
BitMinter	6,451	1.23%
50BTC	6,406	1.23%

# Diğer Fikir Birliği Algoritmaları

- PoW algoritmaları çok enerji harcıyor.
- Daha çevreci yöntemlere ihtiyaçlar var.

# Diger Fikir Birligi Algoritmaları

## PoS: Proof-of-Stake

- PoW gibi işlemsel
- Sistem üzerindeki varlıklarınıza göre
- Örnek: NXT, Peercoin

## PoA: Proof-of-Authority

- Özel ağlar için düşünülmüştür.
- Blok onaylarını sistem yöneticileri yapmaktadır.
- Örnek: POA ( <https://poa.network> )

## PoC: Proof-of-Capacity

- HDD Madenciliği
- Daha çok alanı olan yeni bloğun sahibi olur.
- Örnek: Burstcoin

# Burstcoin



# Alternatif Kripto Para'lar

- Bitcoin dışındaki tüm kripto parabirimlerine genel olarak “Altcoin” denilmektedir.
- Bir çoğu farklı sadece para transferinden fazlasını sunmaktadır.
- Farklı tasarım ilkeleri ile geliştirilmiştir.

Ethereum, Litecoin, Cardano, Zcash, Monero,  
Steem, NXT, IOTA, Dash, Burstcoin, Ripple, ...

# Ethereum

- Vitalik Buterin tarafından 2015 yılında yayınlandı.
- Ethereum Virtual Machine (EVM) isimli bir sanal sistem çalıştırıyor.
- EVM üzerinde “Akıllı kontrat” adı verilen kodlar yazılabilir.
- Yazdığınız kodlar tüm uçbirimler üzerinde çalıştırılıyor.
- “Decentralized apps”

# Ethereum Dapps Uygulamaları

<https://www.stateofthedapps.com>

The screenshot shows the homepage of the State of the DApps website. At the top, there is a browser header with the URL <https://www.stateofthedapps.com>. Below the header, the website's logo 'STATE OF THE DAPPS' is displayed, followed by the tagline 'The curated list of 1.475 decentralized apps'. On the right side of the header, there are navigation links for 'Home', 'DApps', 'Events', and a 'Stay in the loop' button. The main content area features a large, colorful graphic with various DApp icons, including one for 'CRYPTOFIGHTS' and a cat icon. Below this graphic, the title 'EXPLORE DECENTRALIZED APPLICATIONS' is prominently displayed in large, bold letters. A subtitle below it reads: 'Discover the possibilities of the Ethereum blockchain with the definitive registry of DApp projects. [Learn more about DApps](#)'. There are two calls-to-action: a dark button labeled 'Browse the DApps' and a white button labeled 'Submit a DApp'. The background of the page has a gradient from purple to green.

# Kripto Koleksiyonlar

<https://www.cryptokitties.co>

 CryptoKitties

[Start Meow](#) [Marketplace](#)

[FAQs](#) [Blog](#) [More ▾](#)

**Collectible.**  
**Breedable.**  
**Adorable.**

Collect and breed digital cats.

[Start meow](#)

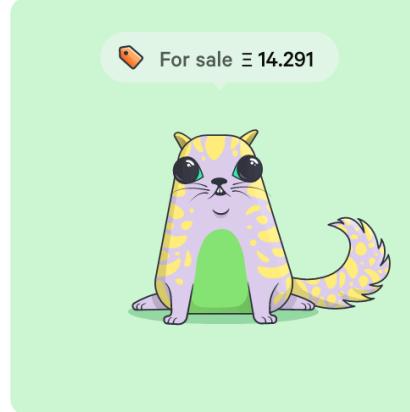
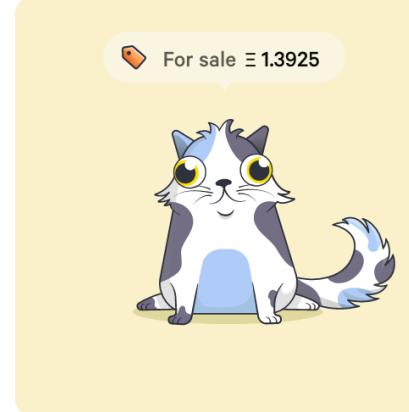
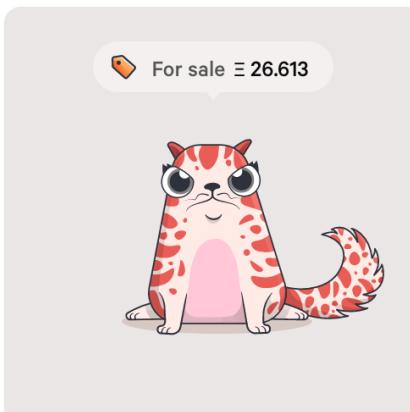
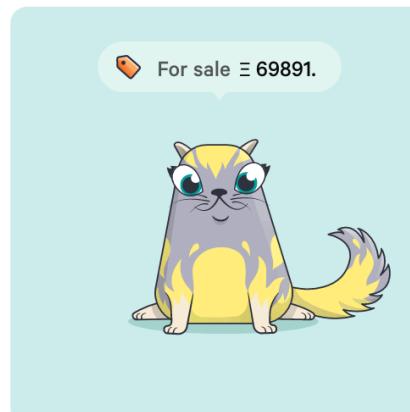
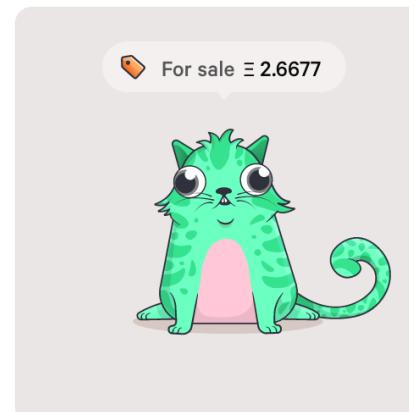


# CryptoKitties

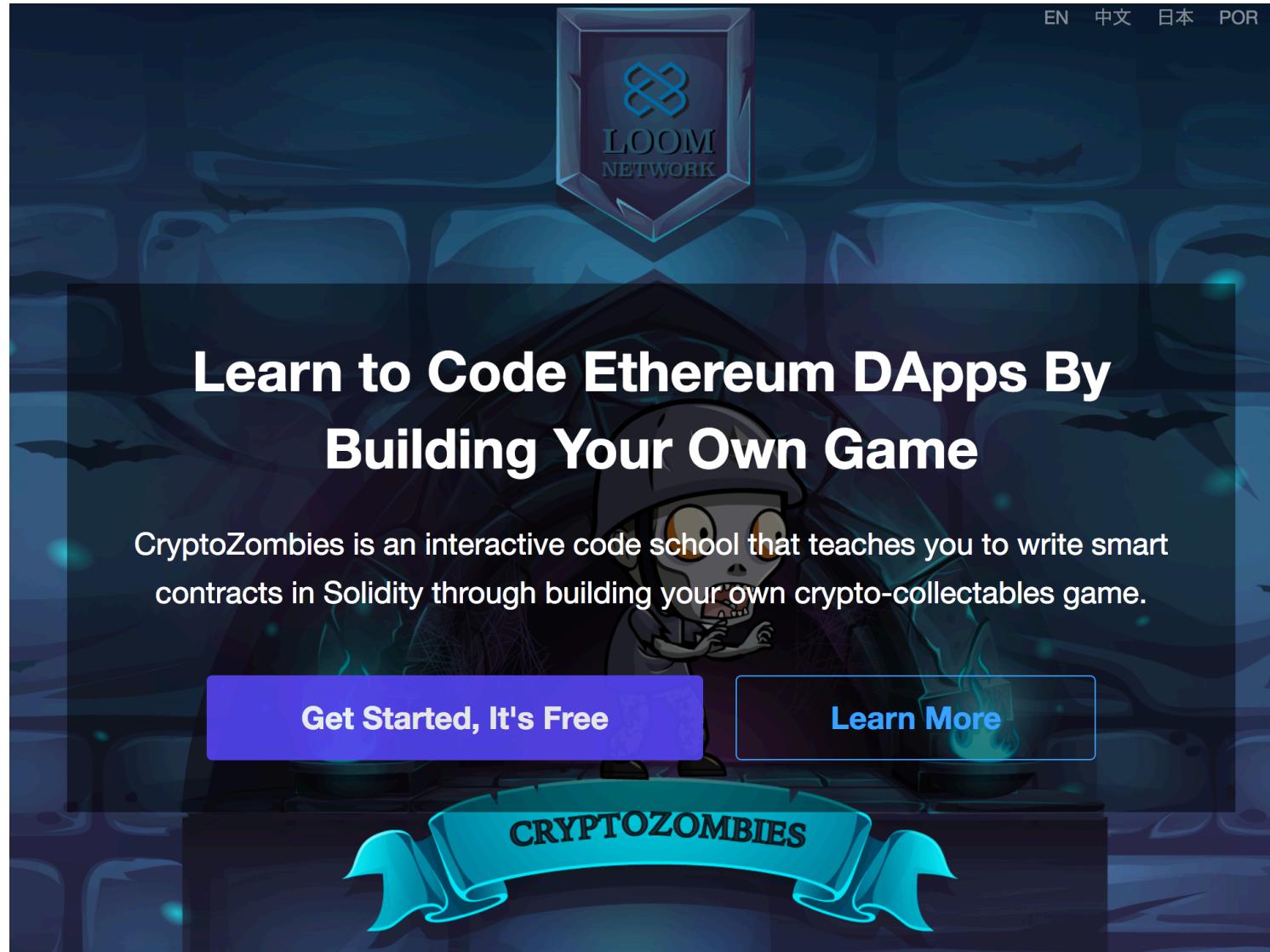
include  for sale  siring  other

sort by Likes ▾ High to low ▾

147315 Kitties

 <p>For sale ⚡ 6.08</p> <p>Kitty 529341 · Gen 4 · Swift 26015</p>	 <p>For sale ⚡ 6</p> <p>Kitty 273346 · Gen 6 · Slow 25812</p>	 <p>For sale ⚡ 14.291</p> <p>Kitty 451610 · Gen 13 · Plodding 18952</p>	 <p>For sale ⚡ 1.3925</p> <p>Kitty 403172 · Gen 5 · Snappy 18264</p>
 <p>For sale ⚡ 8.3798</p> <p>Kitty 503678 · Gen 21 · Slow 18114</p>	 <p>For sale ⚡ 26.613</p> <p>Kitty 504772 · Gen 5 · Swift 18112</p>	 <p>For sale ⚡ 69891.</p> <p>Kitty 345185 · Gen 10 · Slow 18102</p>	 <p>For sale ⚡ 2.6677</p> <p>Kitty 466559 · Gen 11 · Plodding 18099</p>

# CryptoZombies.io



The image shows the landing page of CryptoZombies.io. At the top right, there are language selection links: EN, 中文, 日本, and POR. In the center, there is a logo for LOOM NETWORK, which features a blue infinity symbol above the word "LOOM" and "NETWORK" in a smaller font. Below the logo, the main headline reads: "Learn to Code Ethereum DApps By Building Your Own Game". A cartoon zombie character is visible in the background. Below the headline, a descriptive paragraph states: "CryptoZombies is an interactive code school that teaches you to write smart contracts in Solidity through building your own crypto-collectables game." At the bottom left, a purple button says "Get Started, It's Free". At the bottom right, a white button with a blue border says "Learn More". A blue ribbon banner at the very bottom has the text "CRYPTOZOMBIES" on it.

EN 中文 日本 POR

Learn to Code Ethereum DApps By  
Building Your Own Game

CryptoZombies is an interactive code school that teaches you to write smart contracts in Solidity through building your own crypto-collectables game.

Get Started, It's Free

Learn More

CRYPTOZOMBIES

# Blockzincir Kurumsal Kullanım Alanları

## Permissioned Blockchains

- IBM: Hyperledger
  - Microsoft: Azure Blockchain as a Service (BaaS)
- 
- Veritabanı
    - <https://www.bigchaindb.com>
  - Resmi kayıt yayınılama
    - <https://www.blockcerts.org>
  - Kayıt tutma
  - Varlık yönetimi
  - Kimlik doğrulama
  - Değişim yönetimi

# <https://www.openchain.org>



Developers Wallet

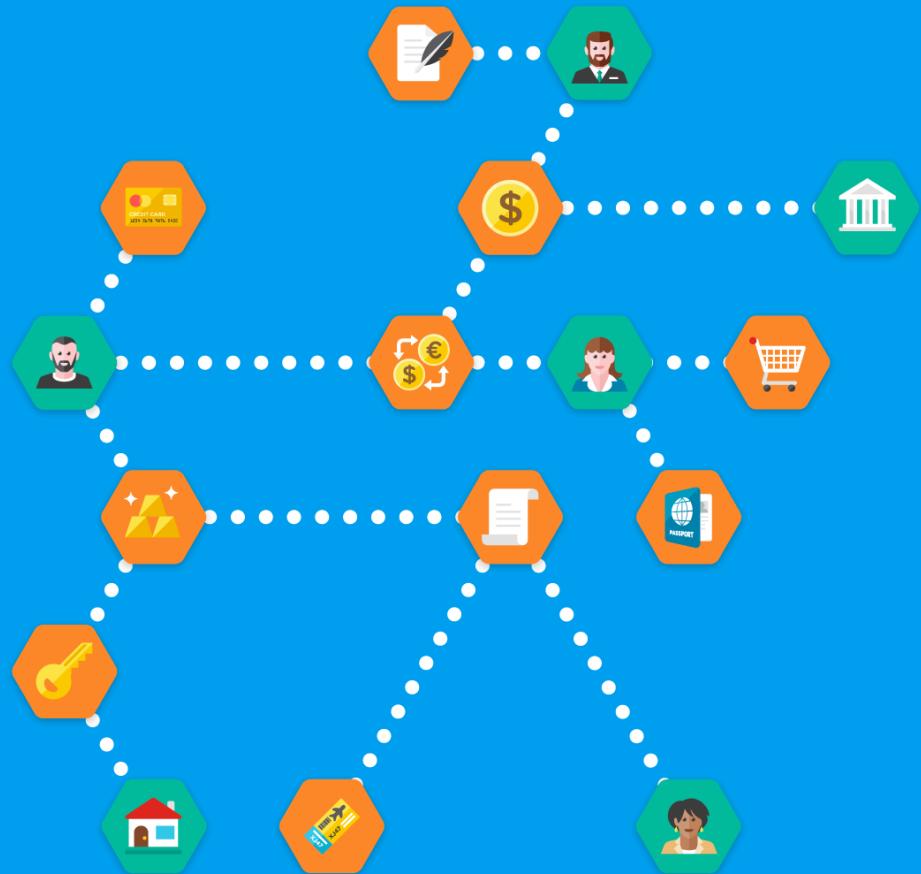
## Blockchain technology for the enterprise

Are you a developer?

Start integrating

Want to try it?

Try our wallet

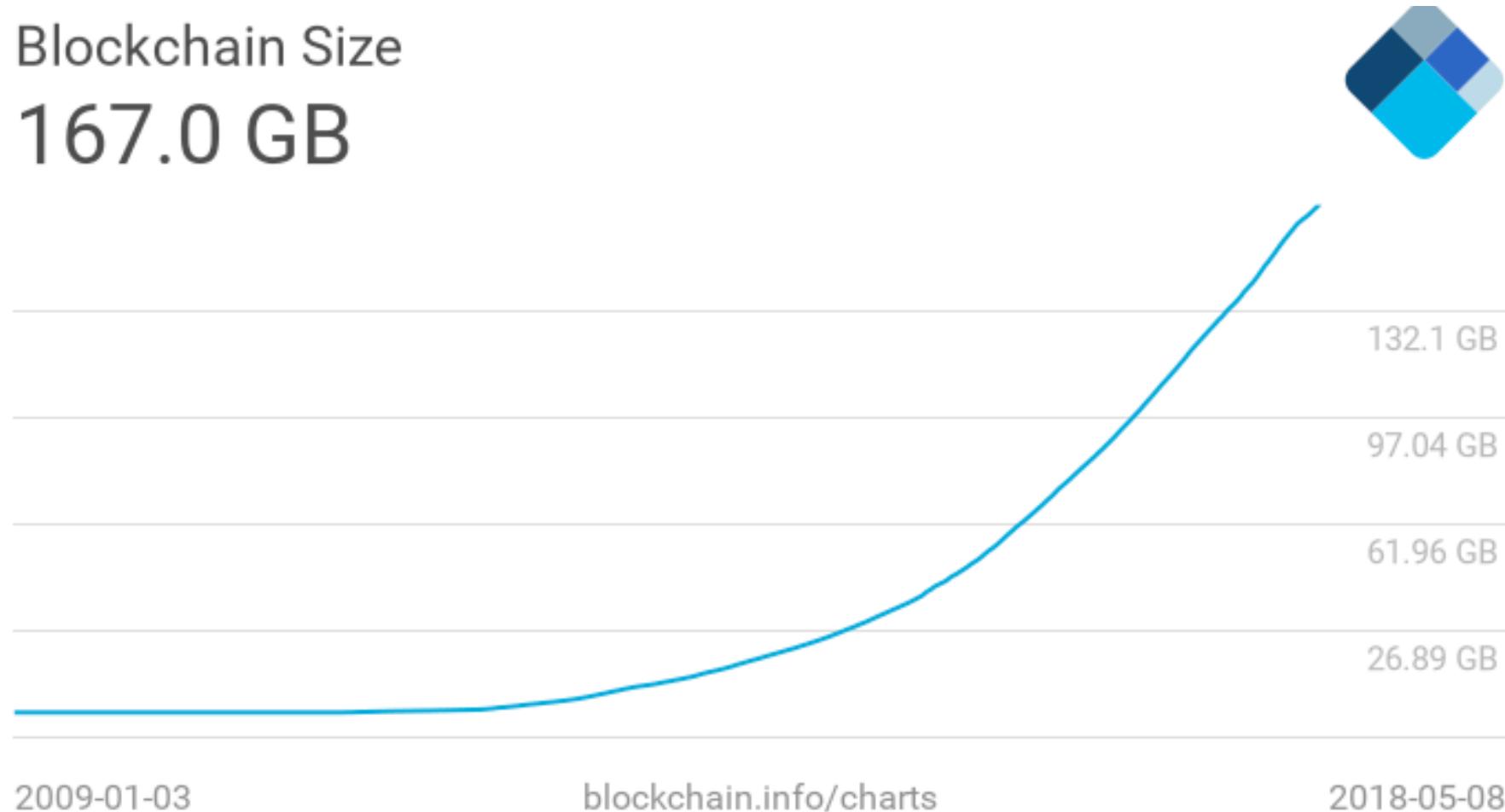


# Blokzincir Araştırma Konuları

- Veritabanı büyüklüğü
- Anlık İşlem Hızı
- Mahremiyet
  - zk-SNARKS
- Yeni fikir birliği algoritmaları
  - Etkin enerji tüketimi
- Blokzincir yapısının farklı alanlarda uygulanabilirliği

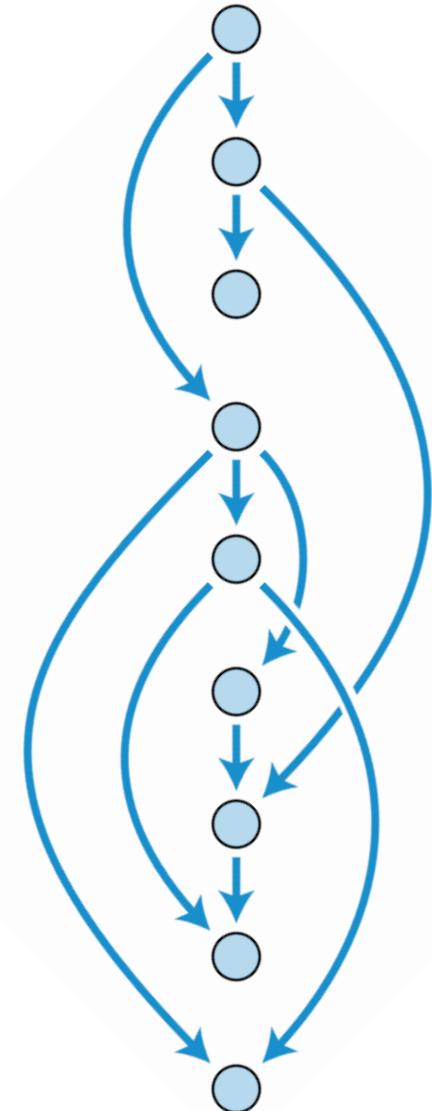
<https://blockchain.info/charts/blocks-size>

Blockchain Size  
167.0 GB



# Blockchain'e Alternatif Yöntemler

- Directed Acyclic Graph
  - IOTA: Tangle
- Lightning Network
  - Blokzincir üzerine geliştirilen bir sistem
  - Anlık işlemler kullanılıyor



# Kendi Blockzincir Tasarımımızı Nasıl Yaparız?

- İhtiyaçlarımızı iyi belirlemek
- Mevcut tasarımları çok iyi anlamak  
(Blokzincir hacker'ı olmak 😊)
- Kriptografik bileşenlere hakim olmak ve doğru ihtiyaç için doğru bileşeni seçmek.

# Do you need a Blockchain?

Karl Wüst\*, Arthur Gervais†

\*karl.wuest@inf.ethz.ch, †arthur.gervais@inf.ethz.ch

Department of Computer Science

ETH Zurich, Switzerland

---

**Abstract**—Blockchain is being praised as a technological innovation which allows to revolutionize how society trades and interacts. This reputation is in particular attributable to its properties of allowing mutually mistrusting entities to exchange financial value and interact without relying on a trusted third party. A blockchain moreover provides an integrity protected data storage and allows to provide process transparency.

In this article we critically analyze whether a blockchain is indeed the appropriate technical solution for a particular application scenario. We differentiate between permissionless (e.g., Bitcoin/Ethereum) and permissioned (e.g. Hyperledger/Corda) blockchains and contrast their properties to those of a centrally managed database. We provide a structured methodology to determine the appropriate technical solution to solve a particular application problem. Given our methodology, we analyze in depth three use cases — Supply Chain Management, Interbank and International Payments, and Decentralized Autonomous Organizations and conclude the article with an outlook for further opportunities.

The remainder of this article is organized as follows. In Section 2 we briefly describe the most important background about blockchain. In Section 3 we provide a structured methodology to identify if a blockchain makes sense, and if yes, which type of blockchain would be appropriate. Based on our methodology, we analyze proposed use cases in detail in Section 4. In Section 5 we review related work in the area, and we conclude the article in Section 6.

## 2 BACKGROUND ON BLOCKCHAIN

In the following section, we detail the required blockchain background and the involved parties. The name blockchain stems from its technical structure — a chain of blocks. Each block is linked to the previous block with a cryptographic hash. A block is a datas-

<http://doyouneedablockchain.com>

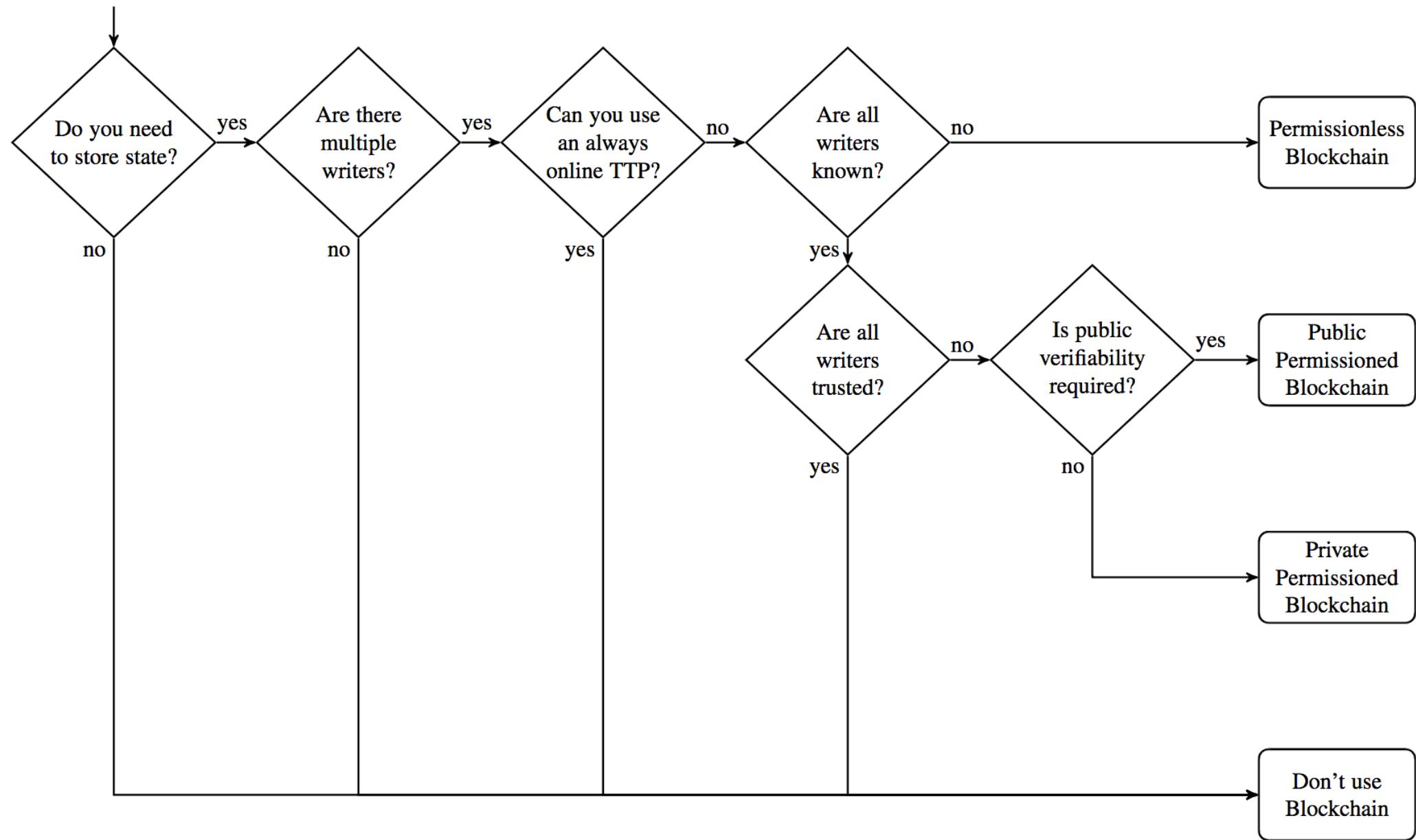
# Do you need a blockchain?

most probably

**NO**

learn more

# Do You Need A Blockchain?



Son.