Blokzincir Üzerine

Halil Kemal Taşkın

İçerik

Bu Sunumda Neler Yok?

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

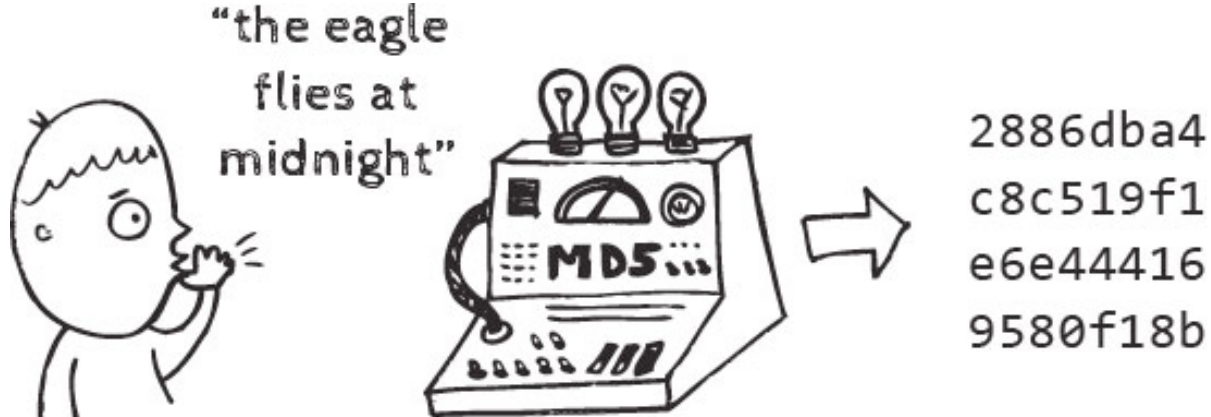
Blokzincir hacker’ı olmak

- ?

Özet fonksiyon

- Kriptografi'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 varsayılır.



Kriptografik Özet fonksiyon

İdeal bir kriptografik özet fonksiyonu şu dört özelliği sağlamalıdır:

- Herhangi bir mesaj için özet hesaplamak kolay olmalıdır.
- Özeti değişmeyecek 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: ~14 milyar yıl ~ **2^{58} saniye**
- Evrendeki yıldızların sayısı ~ **2^{80}**
- Evrendeki tüm atomların sayısı ~ **2^{265}**

- Örnekler:

- 16'lık (Hexadecimal) Gösterim:

  `b2b31a1c59f53e58b2466f3be660a212`

- 2'li (Binary) Gösterim:

  `00110001001100100011001100110100001101010011011000110111001110000011100100110000010000010100001001000011010001000100010101000110`

2^{128} ne kadar büyük olabilir ki?

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

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

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

Blokzincir’in hikayesi

İlk Mesajlar

From: "Satoshi Nakamoto" satoshi@anonymousspeech.com
Sent: Friday, **August 22, 2008** 4:38 PM
To: "Wei Dai" <weidai@ibiblio.org>
Cc: "Satoshi Nakamoto" 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) 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

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

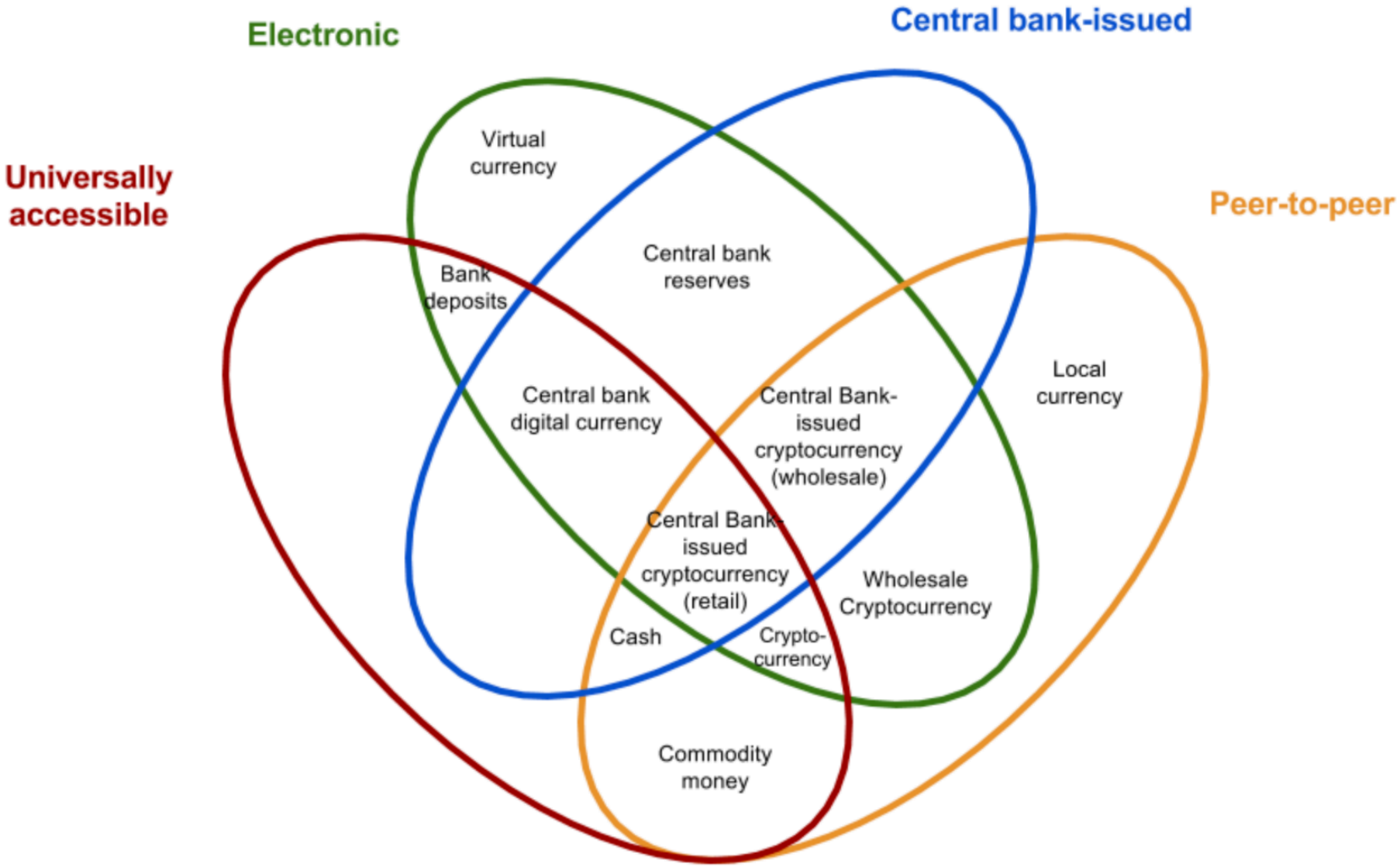
The system is entirely decentralized, without any server or trusted parties. The network infrastructure can support a full range of escrow transactions and contracts, but for now the focus is on the basics of money and transactions.

İlk Mesajlar

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

Blokzincir'in tasarım özellikleri

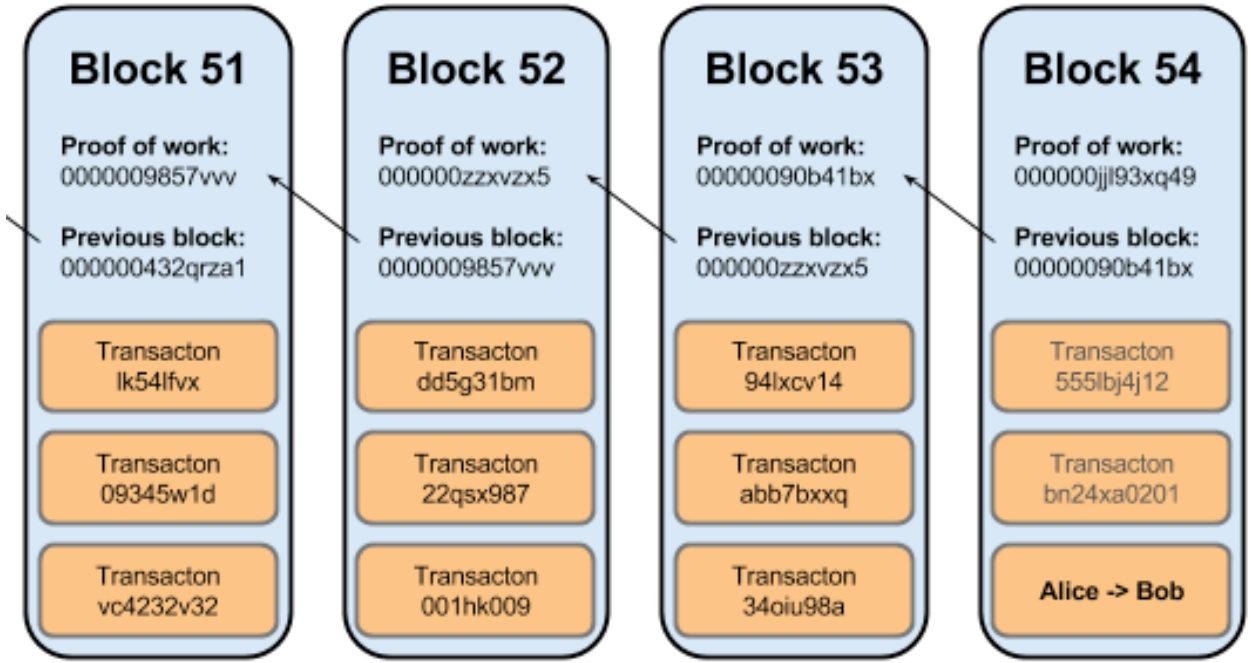
- Tüm kayıtların tutulduğu, açık ve değiştirilmeye dayanıklı bir defter.
- Güvenilir üçüncü tarafa ihtiyaç yok [!]
- Çoğunluğun dürüst olduğu varsayımı üzerine kuruludur. (>%51)
- P2P ağlar üzerinde dağıtık olarak çalışmaya uygun
- Pseudonymity'yi sağlar.
- Anonimlik (Anonymity) sağlamaz [!]

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.

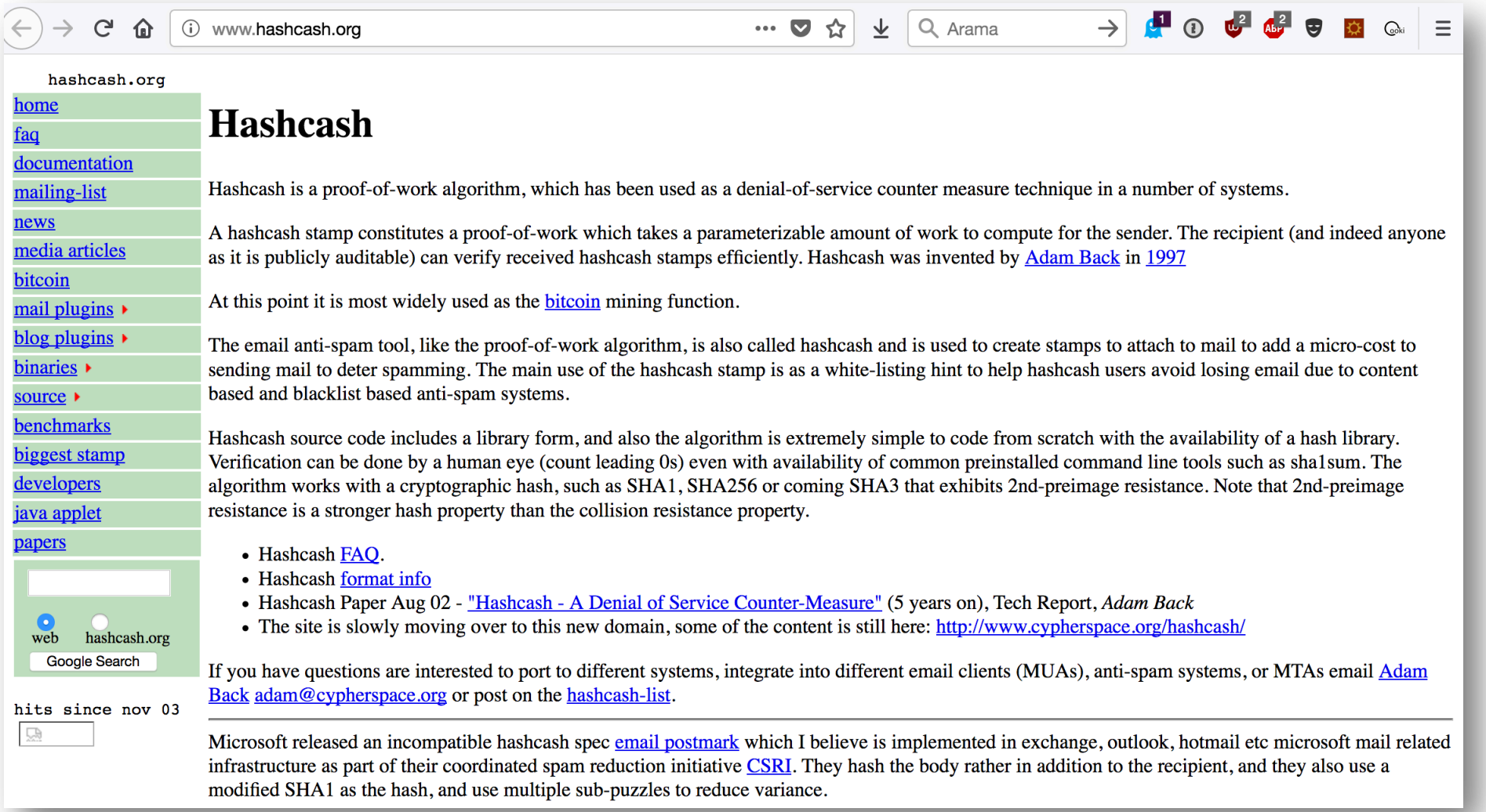
Popüler Örnekleri: Bitcoin, Ethereum, Litecoin, Dogecoin

Artılar: Kesin olarak sonuç veriyor, sorunsuz çalışıyor.

Eksiler: Dünyayı tüketiyor.

Hashcash

Adam Back tarafından 1997 yılında önerilmiştir.



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 üretilecek.
- Blok boyutu en fazla 1MB olabilir.
- Bir blok içine ~2000 işlem sığdırılabilmektedir.
- 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 Kriptografik Özet Fonksiyon tasarımı 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

* https://en.bitcoin.it/wiki/Mining * https://www.cryptocompare.com * https://whattomine.com

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 x 800 kH/s = ~ 2.4 MH/s = 16.41 LTC / Year = 0.13 BTC / Year
Monero average hashrate: 3 x 700 H/s = ~ 2.1 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

* https://bitcointalk.org/index.php?topic=1363187.0

Scrypt is Maximally Memory-Hard

Joël Alwen[1], Binyi Chen[2], Krzysztof Pietrzak[1], Leonid Reyzin[3], and Stefano Tessaro[2]

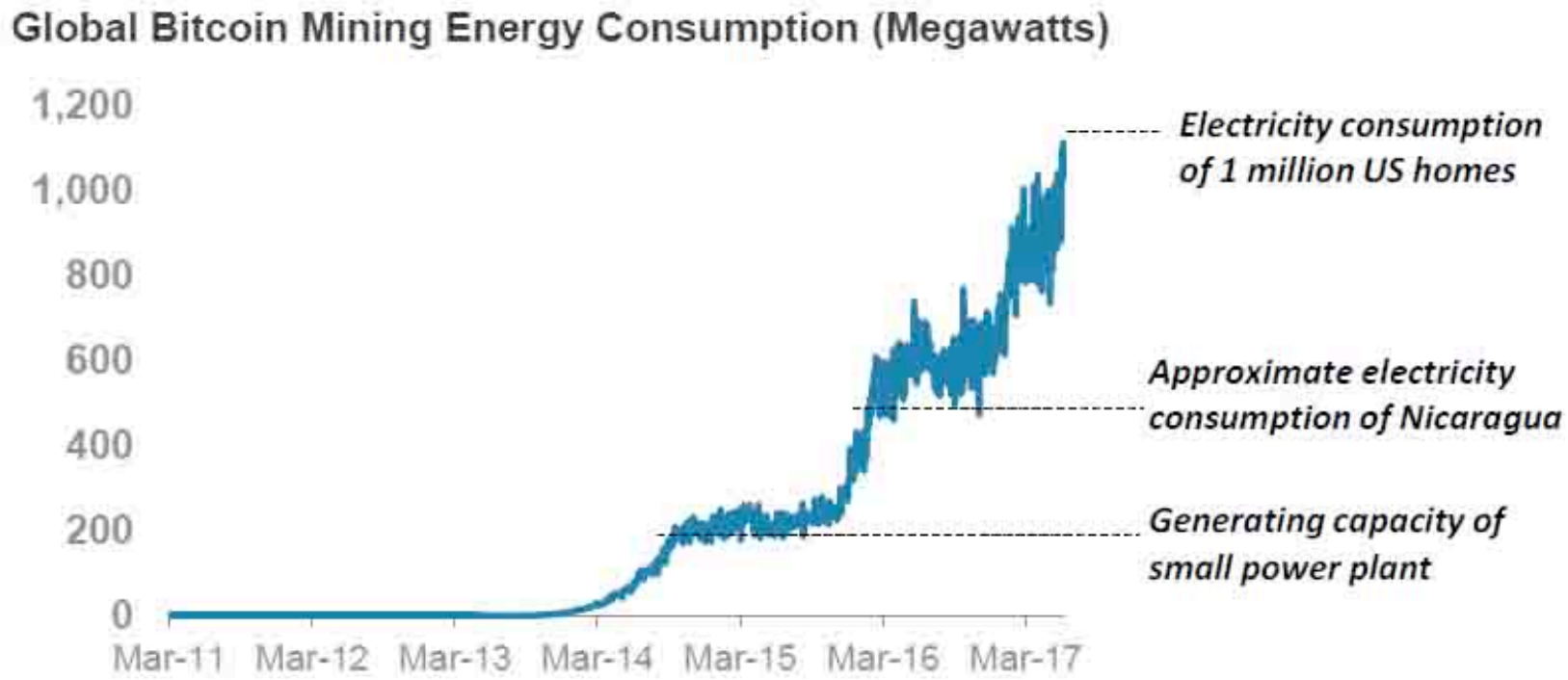
[1] IST Austria
{jalwen,pietrzak}@ist.ac.at
[2] UC Santa Barbara
{binyichen,tessaro}@cs.ucsb.edu
[3] Boston University
reyzin@cs.bu.edu

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

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 boşa 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.

Diğer Fikir Birliği 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.

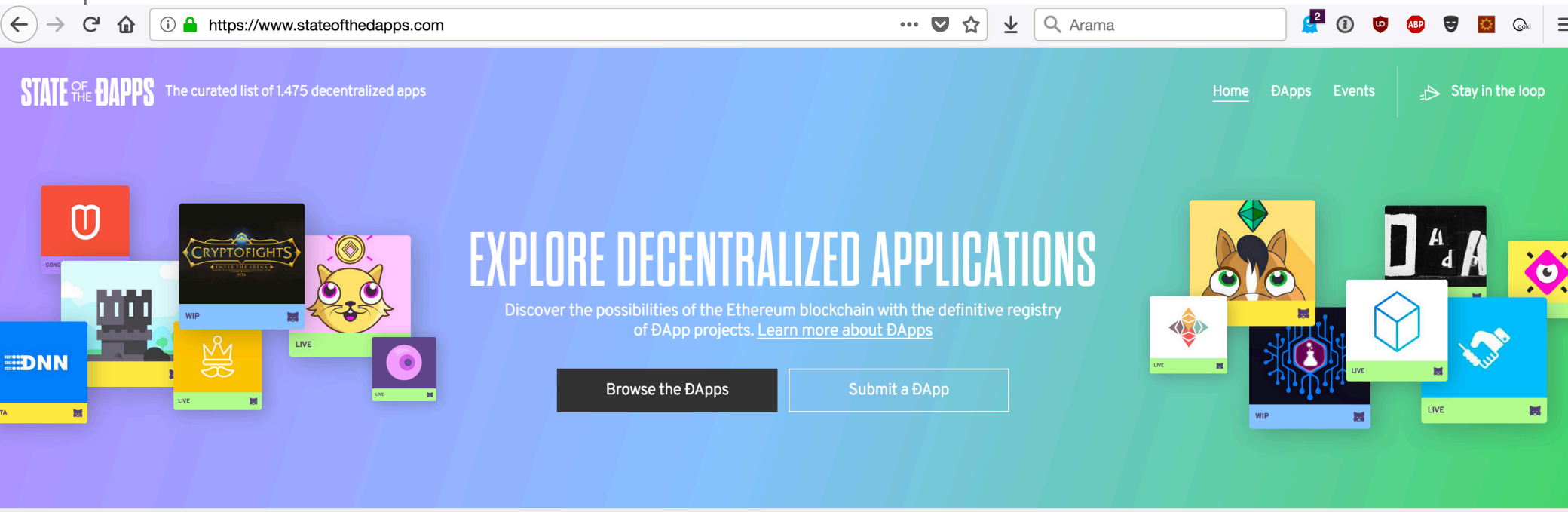
Ethereum, Litecoin, Cardano, Zcash, Monero, Steem, NXT, IOTA, Dash,Burstcoin, Ripple, …

Ethereum

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

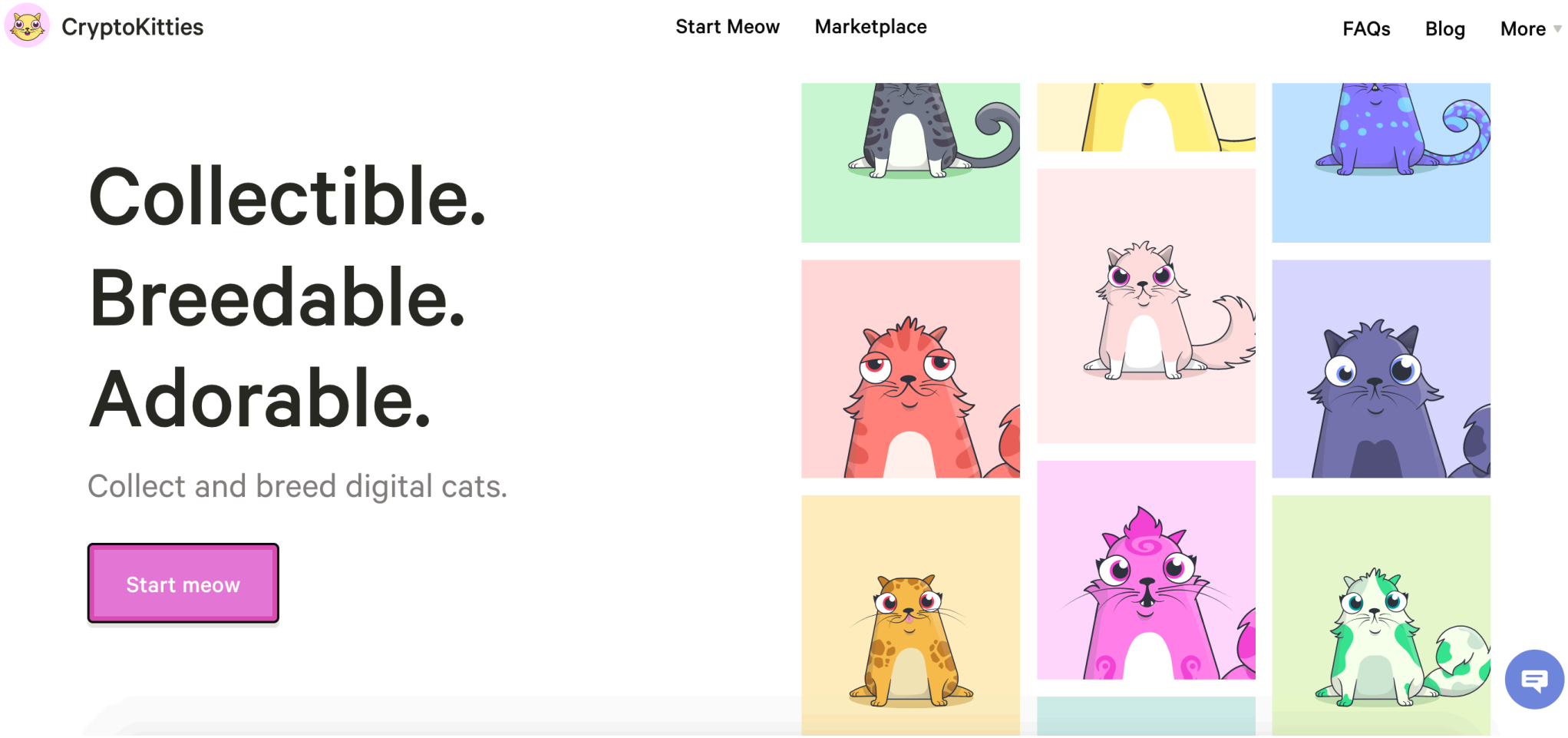
Ethereum Dapps Uygulamaları

https://www.stateofthedapps.com



Kripto Koleksiyonlar

https://www.cryptokitties.co



CryptoKitties

include ☑ for sale ☐ siring ☐ other

sort by Likes ▼ High to low ▼

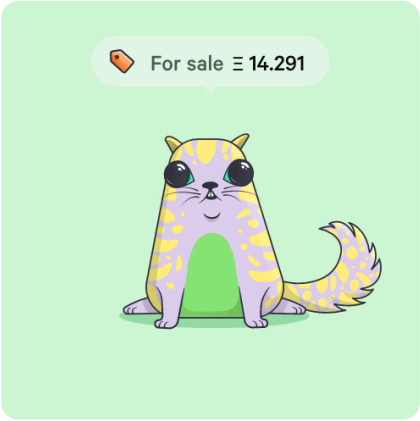
147315 Kitties

Kitty 529341 · Gen 4 · Swift

♡ 26015

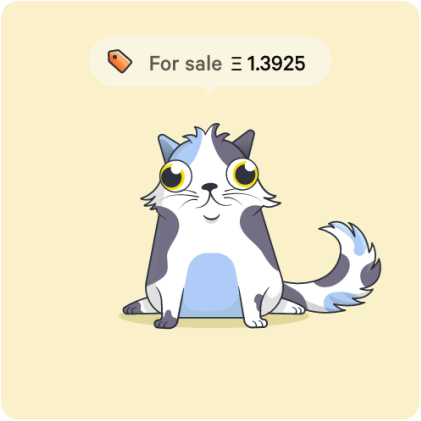
Kitty 273346 · Gen 6 · Slow

♡ 25812



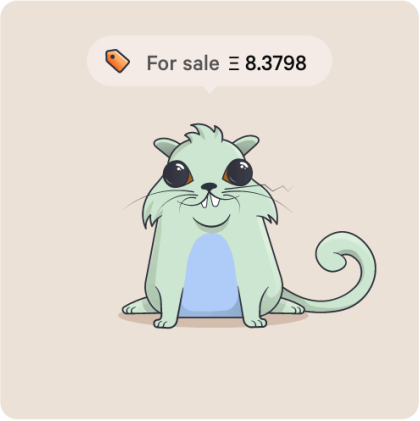
Kitty 451610 · Gen 13 · Plodding

♡ 18952



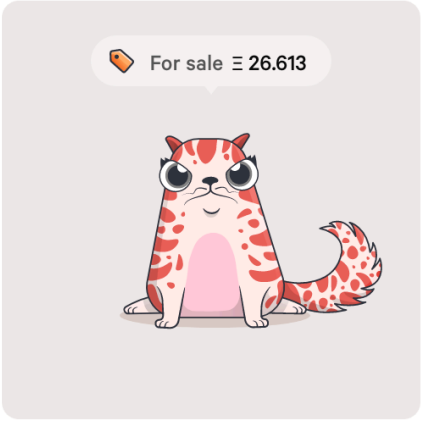
Kitty 403172 · Gen 5 · Snappy

♡ 18264



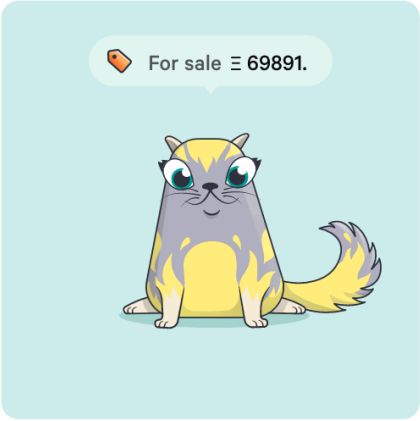
Kitty 503678 · Gen 21 · Slow

♡ 18114



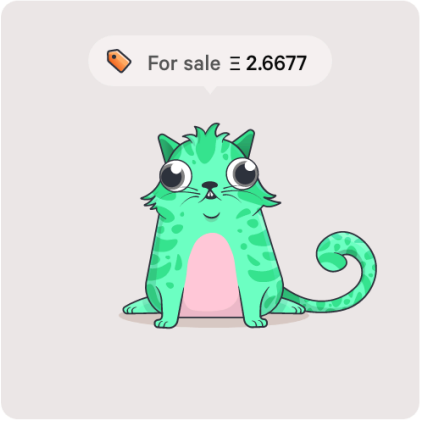
Kitty 504772 · Gen 5 · Swift

♡ 18112



Kitty 345185 · Gen 10 · Slow

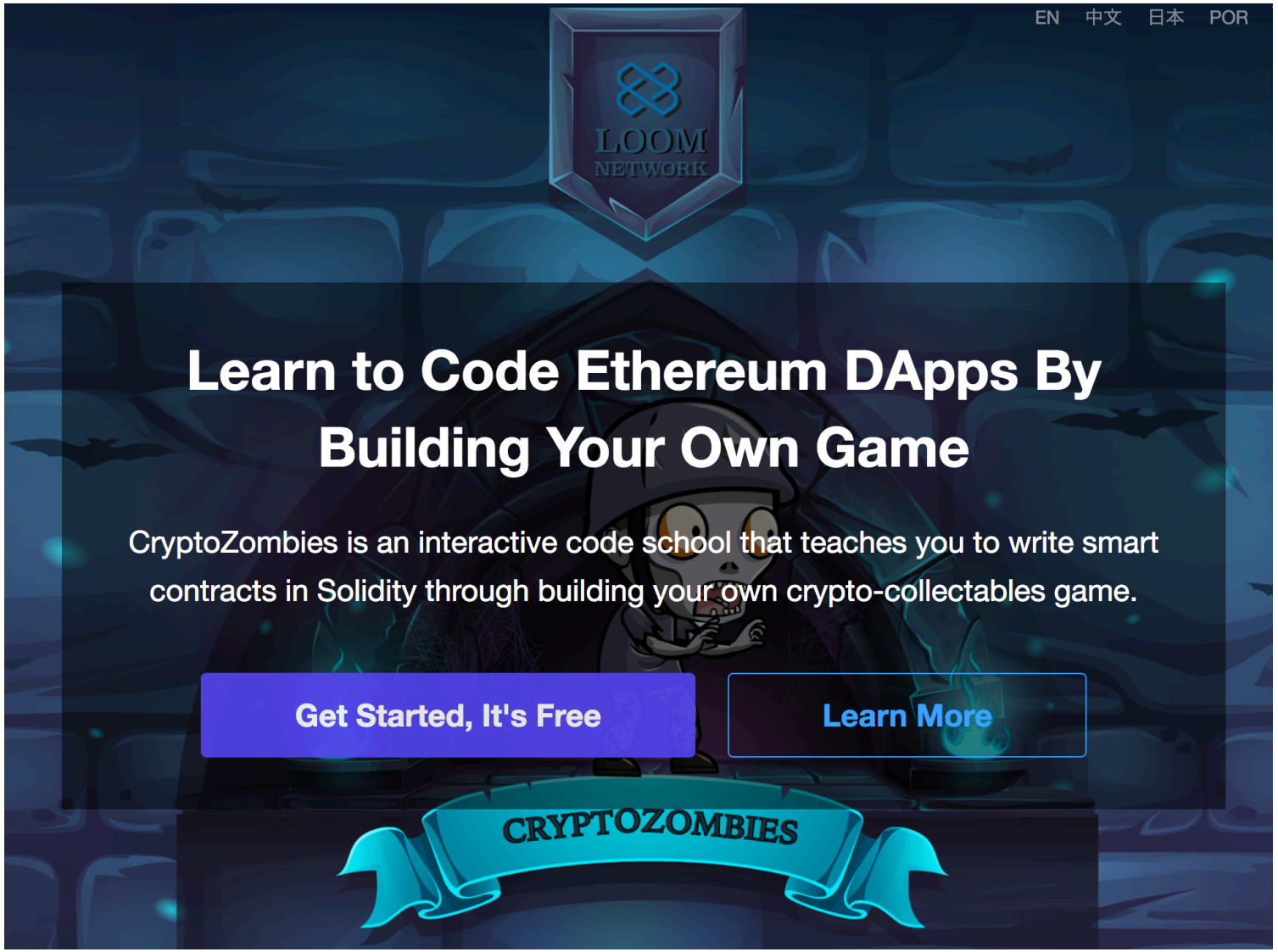
♡ 18102



Kitty 466559 · Gen 11 · Plodding

♡ 18099

CryptoZombies.io



Blockzincir Kurumsal Kullanım Alanları

Permissioned Blockchains

- IBM: Hyperledger
- Microsoft: Azure Blockchain as a Service (BaaS)

- Veritabanı
  - https://www.bigchaindb.com
- Resmi kayıt yayınlama
  - https://www.blockcerts.org
- Kayıt tutma
- Varlık yönetimi
- Kimlik doğrulama
- Değişim yönetimi

https://www.openchain.org

openchain

Developers Wallet

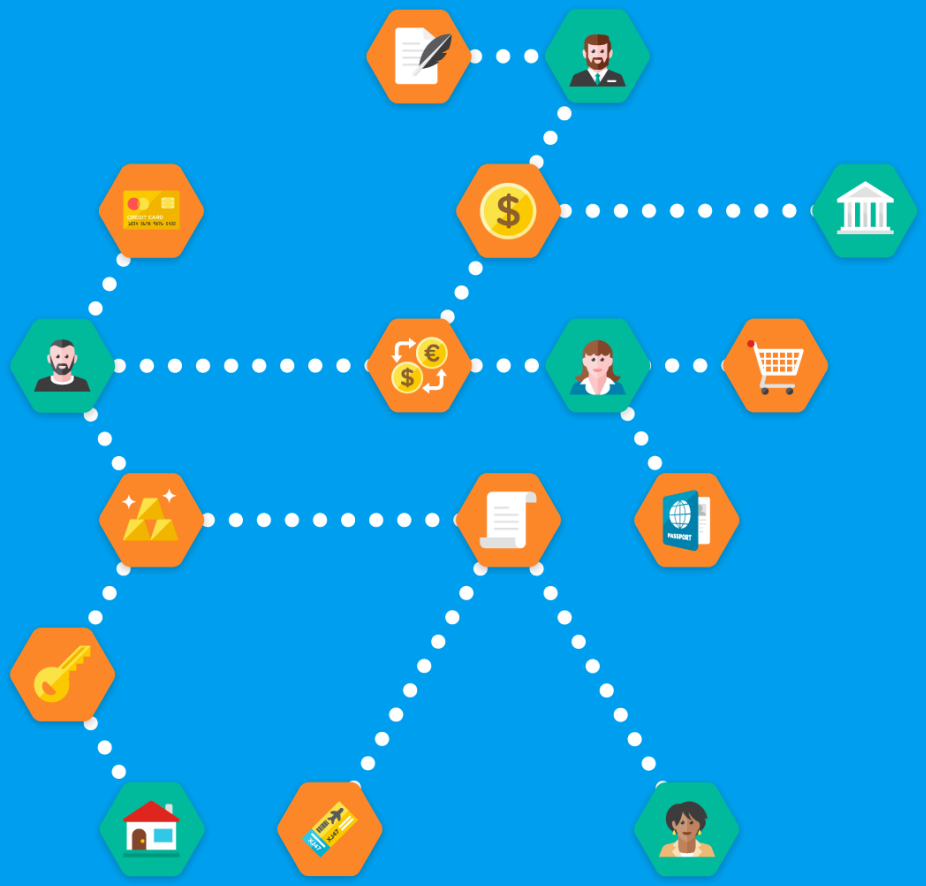
Blockchain technology for the enterprise

Are you a developer?

Start integrating

Want to to try it?

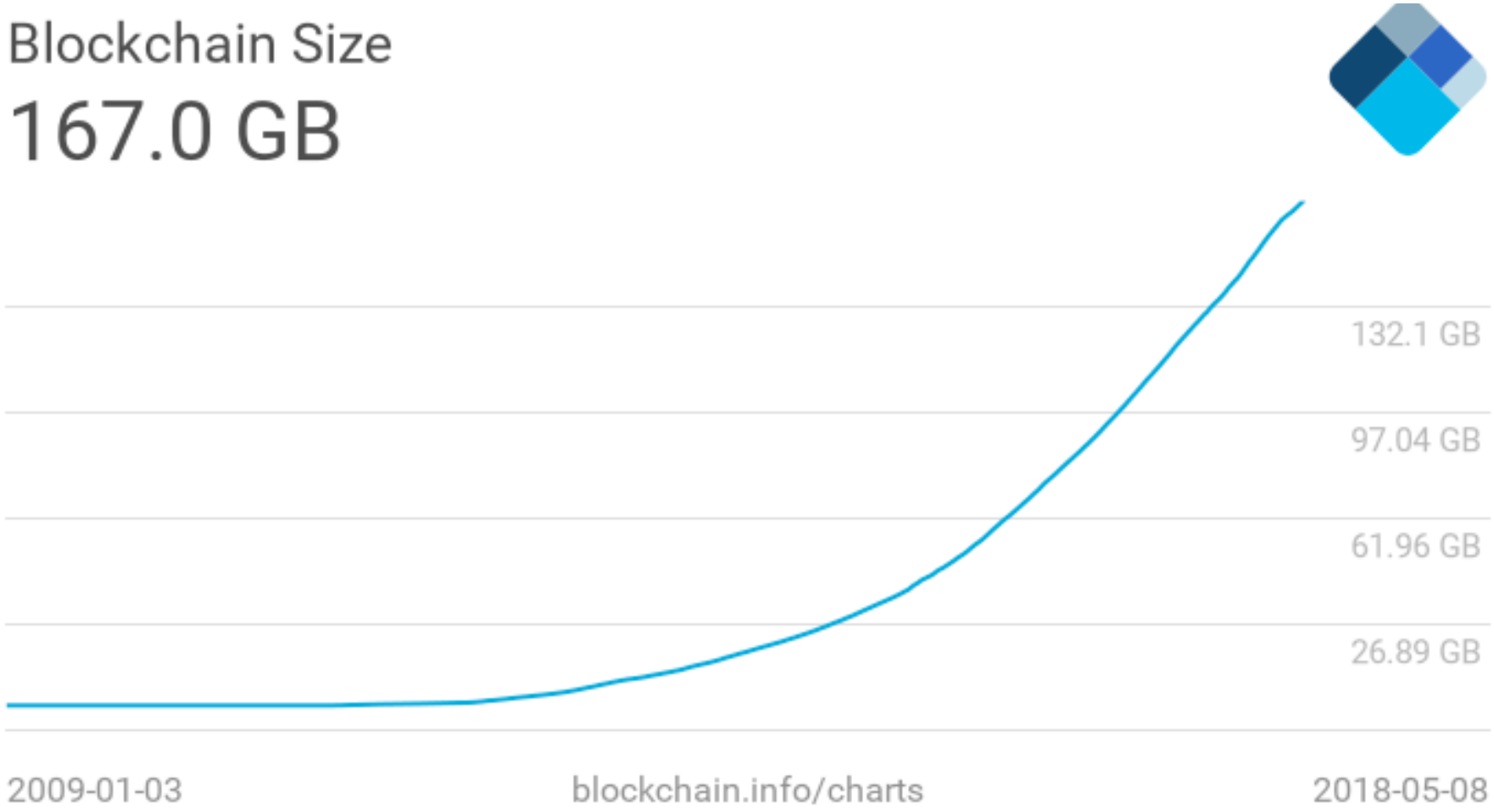
Try our wallet



Blokzincir Araştırma Konuları

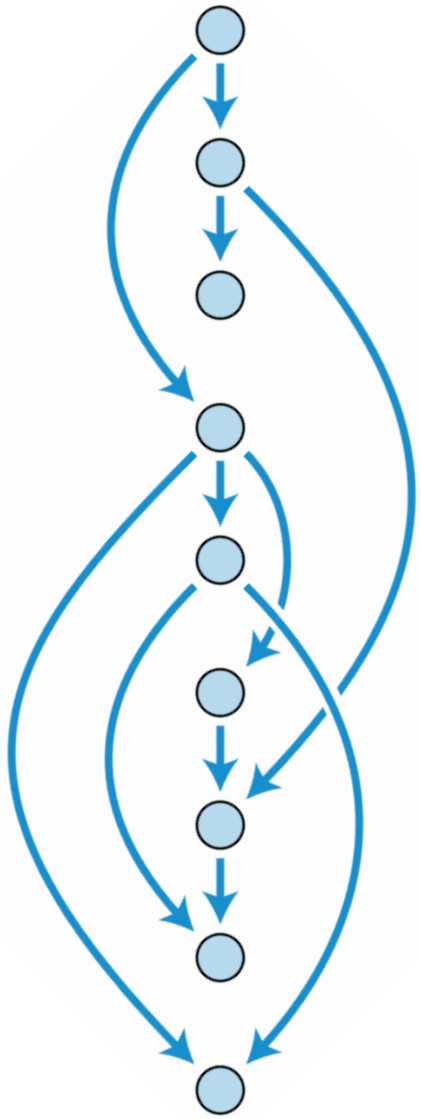
- Veritabanı büyüklüğü
- Anlık İşlem Hızı
- Mahremiyet
  - **zk-SNARKS**
- Yeni fikir birliği algoritmaları
  - Etkin enerji tüketimi
- Blokzincir yapısının farklı alanlarda uygulanabilirliği

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



Blockchain’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

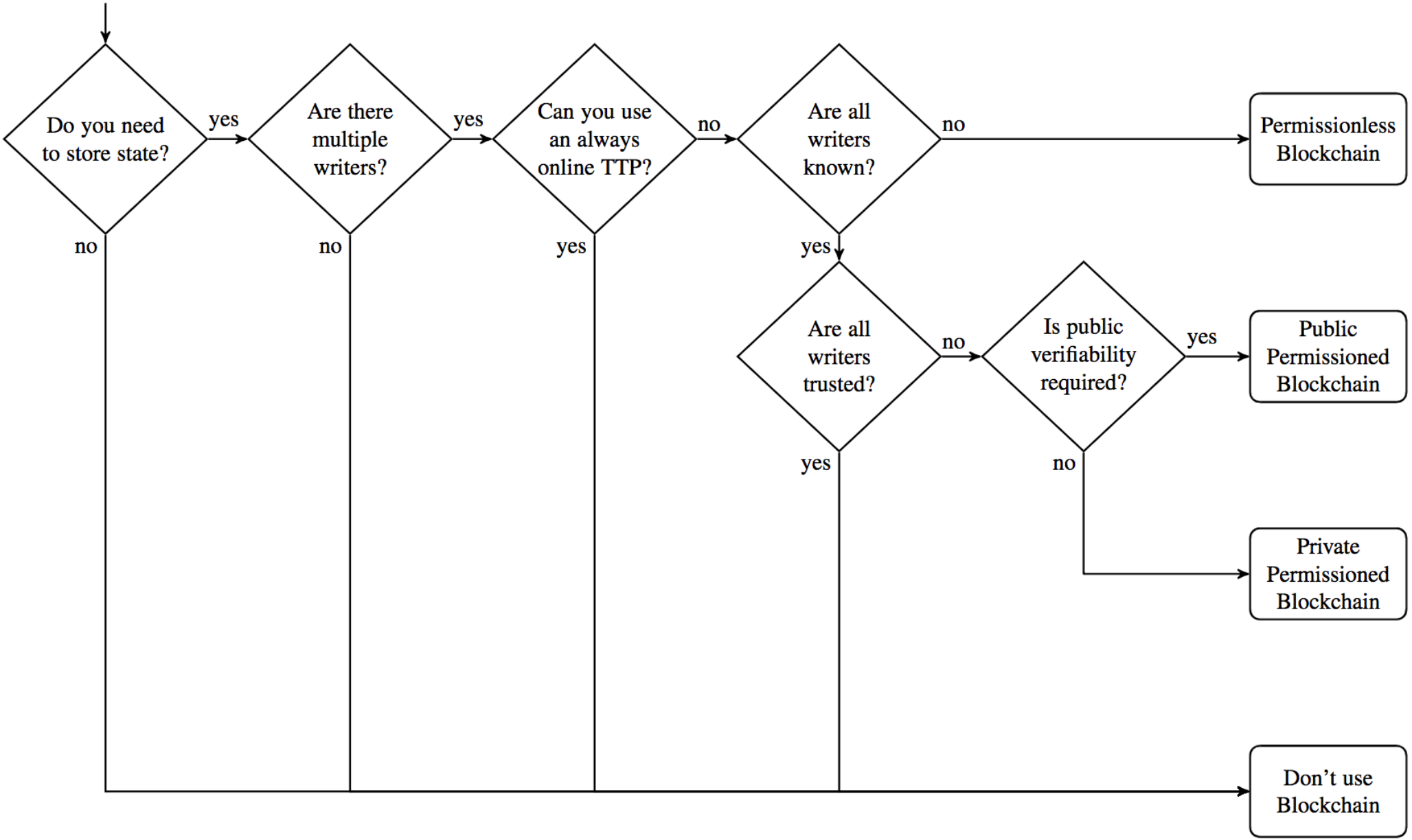
Do you need a
blockchain?

most probably
NO

learn more

Based on Wüst, Karl, and Arthur Gervais. "Do you need a Blockchain?" *IACR Cryptology ePrint Archive* 2017 (2017): 375.

Do You Need A Blockchain?



Son.