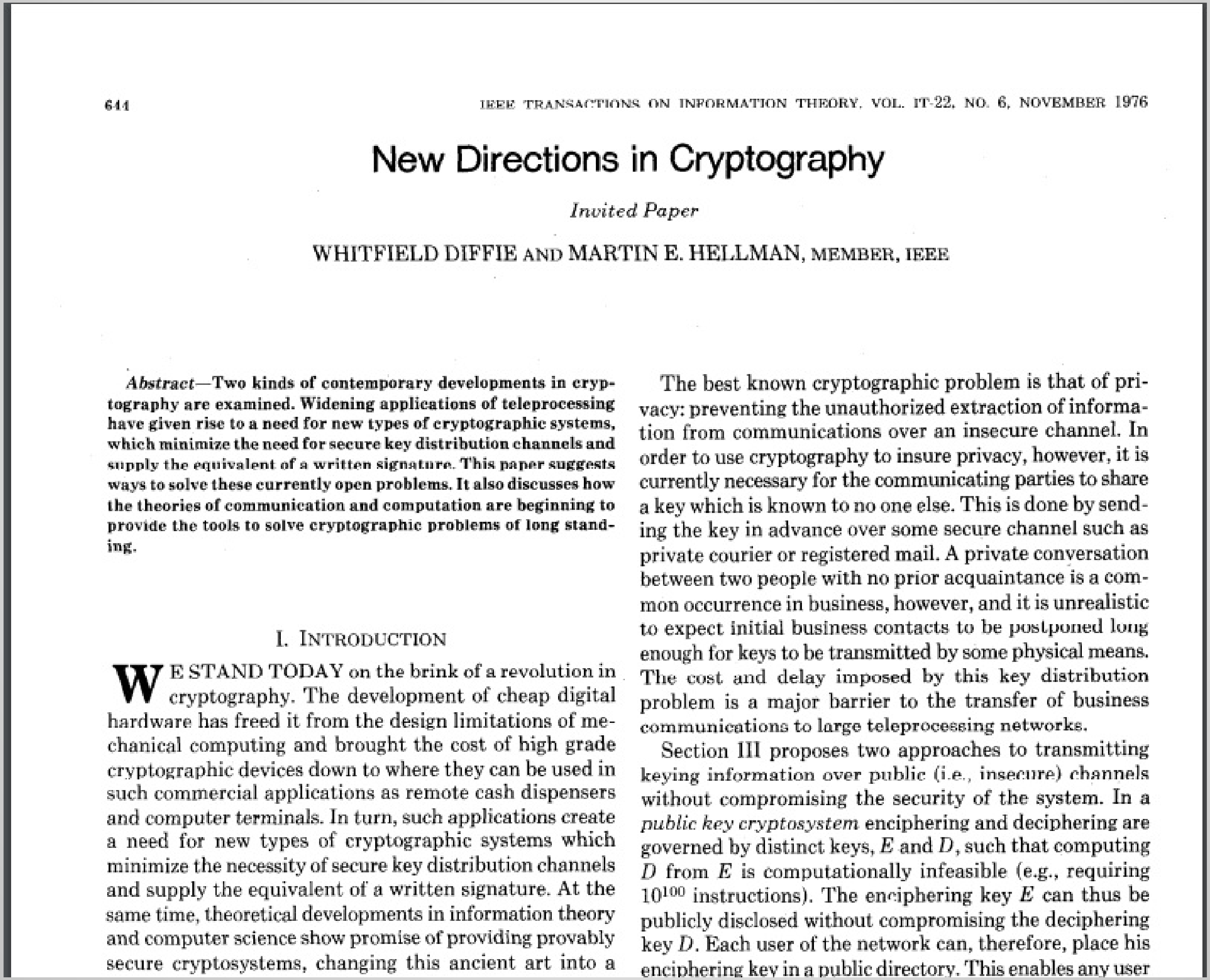
Giriş

TÜBİTAK

BU SUNUMDAKİ HİÇBİR BİLGİ KURUMUN RESMİ DÜŞÜNCELERİNİ YANSITMAMAKTADIR

SUNUMA KONU OLAN HER TÜRLÜ BİLGİ TAMAMEN INTERNET VE ÇEŞİTLİ KAYNAKLARDAN DERLENEREK SUNULMUŞTUR

Bitcoin Öncesi



New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

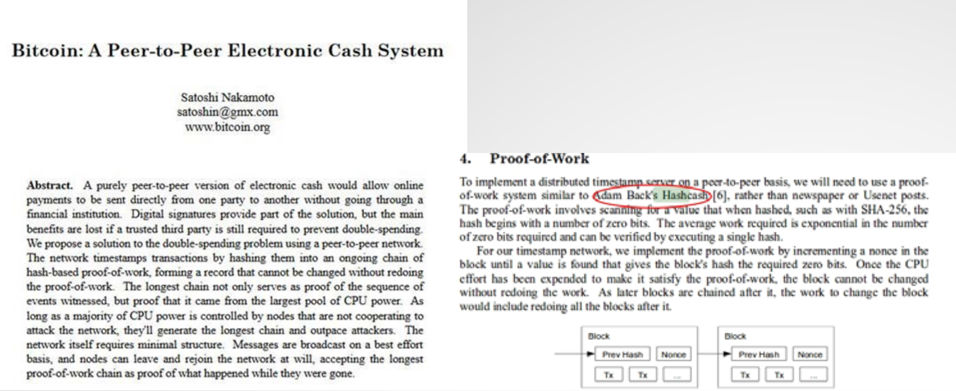
I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user

Bitcoin’in Kısa Tarihi



Bitcoin: A Peer-to-Peer Electronic Cash System

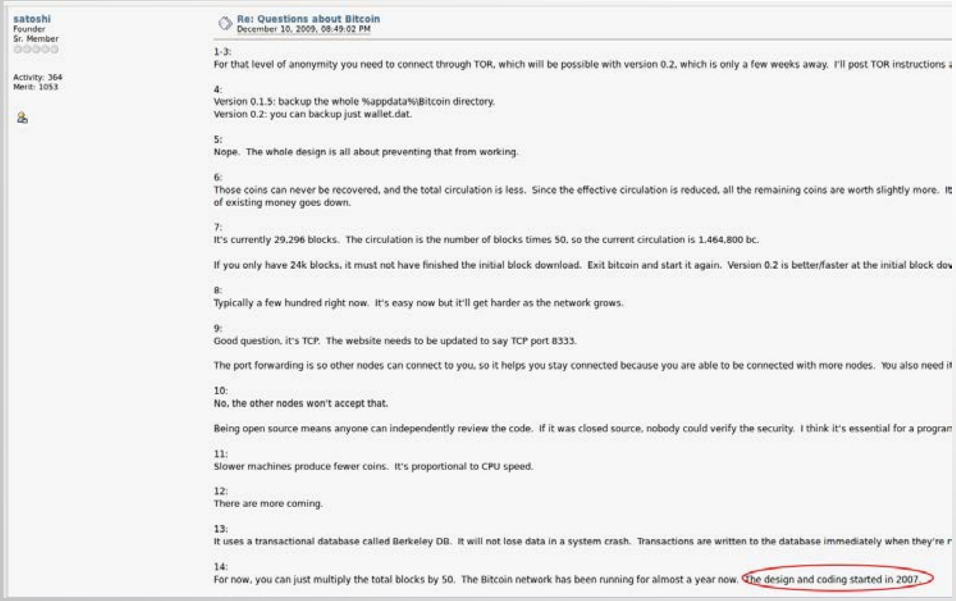
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



satoshi
Founder
Sr. Member

Activity: 364
Merit: 1053

Re: Questions about Bitcoin
December 10, 2009, 08:49:02 PM

1-3:
For that level of anonymity you need to connect through TOR, which will be possible with version 0.2, which is only a few weeks away. I'll post TOR instructions a

4:
Version 0.1.5: backup the whole %appdata%\Bitcoin directory.
Version 0.2: you can backup just wallet.dat.

5:
Nope. The whole design is all about preventing that from working.

6:
Those coins can never be recovered, and the total circulation is less. Since the effective circulation is reduced, all the remaining coins are worth slightly more. It
of existing money goes down.

7:
It's currently 29,296 blocks. The circulation is the number of blocks times 50, so the current circulation is 1,464,800 bc.

If you only have 24k blocks, it must not have finished the initial block download. Exit bitcoin and start it again. Version 0.2 is better/faster at the initial block dow

8:
Typically a few hundred right now. It's easy now but it'll get harder as the network grows.

9:
Good question, it's TCP. The website needs to be updated to say TCP port 8333.

The port forwarding is so other nodes can connect to you, so it helps you stay connected because you are able to be connected with more nodes. You also need it

10:
No, the other nodes won't accept that.

Being open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a progran

11:
Slower machines produce fewer coins. It's proportional to CPU speed.

12:
There are more coming.

13:
It uses a transactional database called Berkeley DB. It will not lose data in a system crash. Transactions are written to the database immediately when they're r

14:
For now, you can just multiply the total blocks by 50. The Bitcoin network has been running for almost a year now. The design and coding started in 2007.

- **2007** Bitcoin kodu geliştirildi

- **5 Ekim 2008** *nakamoto2* sourceforge’a register oldu (User ID: 2238460)

  10 Aralık 2008 s_nakamoto, yine Satoshi Nakamoto ismiyle, register oldu? - User ID: 2321442

- **31 Ekim 2008** *metzdowd.com*’daki **cypherpunks** Kriptografi E-posta listesinde (cryptography@metzdowd.com) **Bitcoin makalesi** yayınlandı

- **18 Agustos 2008**, Satoshi tarafından bitcoin.org Web sitesi register edildi
  - anonymousspeech.com (Japonya) üzerinden prepaid kart’la
  - **4 Ocak 2008**’de is bitcoin.com register edildi

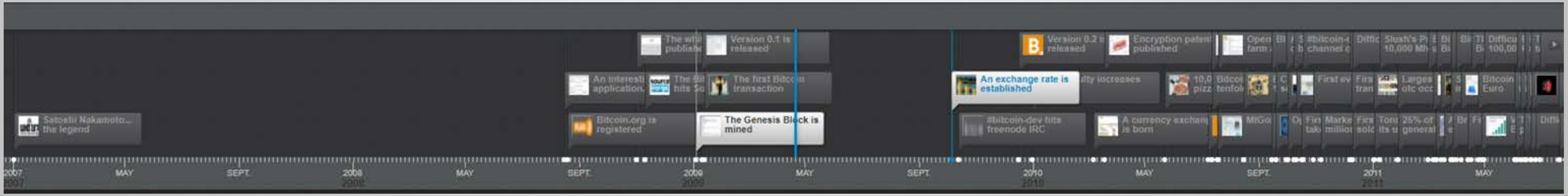
Bitcoin’in Kısa Tarihi

TÜBİTAK

- **17 Kasım 2009**’da sourceforge tarafından host edilen ancak şimdi ulaşılamayan bir adreste **http://bitcoin.sourceforge.net/boards/index.php**, **Bitcoin forumu** oluşturuldu
    - ***sirius (Martti Malmi)*** tarafından hosting sağlanmaya başlandıktan sonra forum forum.bitcoin.org’e taşındı
    - *bitcoin.org domain ismi Satoshi’den sirius’a transfer edildi*
    - Forum Temmuz 2011’de bitcointalk.org’a taşındı
    - *Sirius → bitcointalk.org’un sahibi*

- **Ocak 2009**’da Bitcoin yazılımı paylaşılmadan önce üzerinde bir seri test gerçekleştirildi

- **3 Ocak 2009**’da ilk blok kazıldı



Bitcoin’in Kısa Tarihi

- **9 Ocak 2009**’da Sourceforge’da Bitcoin güncellenmiş 0.1 sürümü yayınlandı
- **12 Ocak 2009**’da 170. blokta kayıtlı ilk transfer *Satoshi → Hal Finney* gerçekleşti

2 yıl Nakamoto ismi ile yazışmalardan sonra Aralık 2010’da projenin yönetimini **Gavin Andresen**’e devrederek ortadan kayboldu

- **23 Nisan 2011**’de tekrar ortaya çıkan Nakamoto, Mike Hearn isimli yazılımcıya attığı E-postada “***Başka konularla uğraşmaya başladığını ve Bitcoin’in Gavin’in ve diğer herkesin elinde iyi olduğunu***” bildirdi

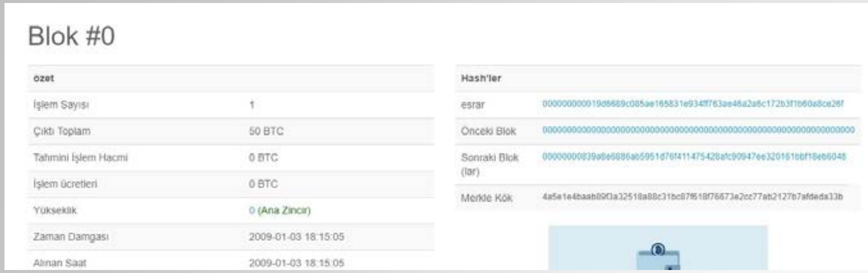
Windows 95 piyasaya sürüldükten sonra Bill Gates’in veya
İlk iPhone piyasaya çıktıktan sonra Steve Jobs’un ortadan kaybolması gibi…

İlk işlem 2013’te bir pizza alımı için

Gavin 2012’de Bitcoin Vakfı’nı hayata geçirdi ve 8 Nisan 2014’te sorumluluklarını **Wladimir J. van der Laan**’a devretti…

- **Haziran 2001,** Wikileaks Bitcoin’le bağış kabul etmeye başladı
- **Şubat 2012**, ***Bitcoin Magazine*** yayın hayatına başladı...

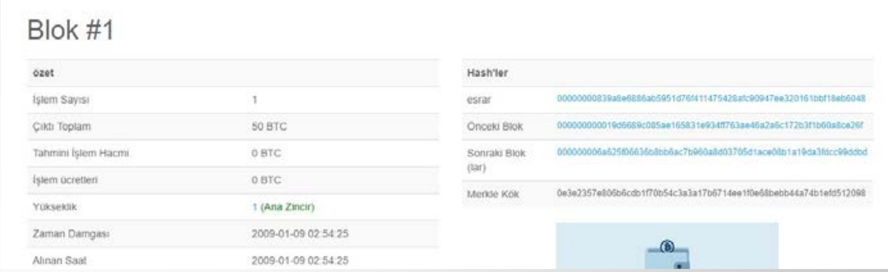
Bitcoin’in Kısa Tarihi, GENESIS



Blok #0

özet	
İşlem Sayısı	1
Çıktı Toplam	50 BTC
Tahmini İşlem Hacmi	0 BTC
İşlem ücretleri	0 BTC
Yükseklik	0 (Ana Zincir)
Zaman Damgası	2009-01-03 18:15:05
Alınan Saat	2009-01-03 18:15:05

Hash'ler	
esrar	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Önceki Blok	0000000000000000000000000000000000000000000000000000000000000000
Sonraki Blok (lar)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Kök	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b



Blok #1

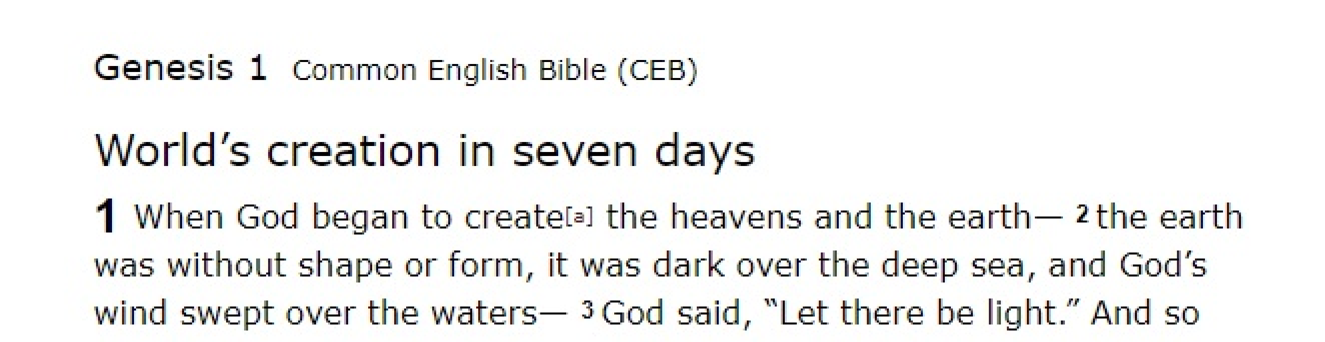
özet	
İşlem Sayısı	1
Çıktı Toplam	50 BTC
Tahmini İşlem Hacmi	0 BTC
İşlem ücretleri	0 BTC
Yükseklik	1 (Ana Zincir)
Zaman Damgası	2009-01-09 02:54:25
Alınan Saat	2009-01-09 02:54:25

Hash'ler	
esrar	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Önceki Blok	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Sonraki Blok (lar)	000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd
Merkle Kök	0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098

3 Ocak 2009

9 Ocak 2009

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"



Genesis 1 Common English Bible (CEB)

World’s creation in seven days

1 When God began to create[a] the heavens and the earth— 2 the earth was without shape or form, it was dark over the deep sea, and God’s wind swept over the waters— 3 God said, “Let there be light.” And so

«Tominaga Nakamoto»

Mukishinron → Ateizmin Japon versiyonu

Bitcoin'in Kısa Tarihi

Gavin Andresen

VRML 2.0 spesifikasyonunun yazarlarından

"After **graduating from Princeton University in 1988**, Andresen began…"

Shinichi Mochizuki, d. 1969

Japon Matematikçi, Sayı Teorisi ve Geometri

"Phillips Exeter Academy and graduated in 1985. **He entered Princeton University as an undergraduate at age 16 and graduated salutatorian in 1988.** He then…"

Profil, Satoshi Nakamoto

- Bilimadamı nitelikleri
- Kriptografi konusunda son derece yetenekli
- Ender bulunacak bir hayal gücü
- 2012’deki P2P Foundation profiline göre
  - 5 Nisan 1975, 37 yaşında
  - Japonya Doğumlu
- Mükemmel İngiliz aksanı ile yazan

Nakamoto Neden Anonim Kalmak İstedi?

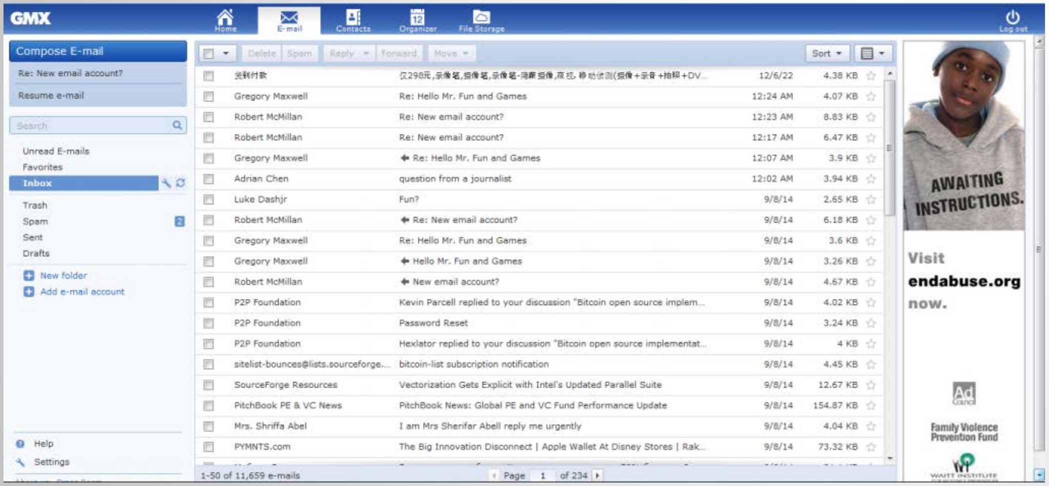
- Bitcoin’in yasadışı amaçlar için istismar edilmesinden rahatsız oldu (silkroad)
- Amerikan otoritelerinin kripto paralar konusunda gösterebilecekleri tepkiden tedirgin oldu
- 1 milyon Bitcoin’e sahip olduğu iddiası

Satoshi → Akıllı
Naka → İçinde
Moto → Kurum

Satoshi → Küllerinden doğan
Nakamoto → Merkezi

Profil, Satoshi Nakamoto

- Satoshi Nakamoto’nun kullandığı **satoshin@gmx.com** adresli E-posta hesabı kendisini Jeffrey ismi ile tanıtan bir hacker tarafından 2014 yılında hack’lendi
- 2011 yılına kadar giden E-posta mesajları
- Jeffrey Tor tarayıcısını gerektiği şekilde kurmayan Satoshi’nin 2010 yılında E-posta hesabını kullanması esnasında IP’sini sızdığını iddia ediyordu
- Hacket 25BTC’lik ödeme karşılığında Satoshi’nin sırlarını paylaşmayı teklif etti
- Aynı hacker tarafından daha önce eklenen Roger Ver bu hacker’ı yakalanmasını sağlayanlara 37,6BTC’lik ödül vadetti.



货到付款	仅298元,录像笔,摄像笔,录像笔-隐蔽摄像,夜视, 移动侦测(摄像+录音+拍照+DV...	12/6/22	4.38 KB
Gregory Maxwell	Re: Hello Mr. Fun and Games	12:24 AM	4.07 KB
Robert McMillan	Re: New email account?	12:23 AM	8.83 KB
Robert McMillan	Re: New email account?	12:17 AM	6.47 KB
Gregory Maxwell	← Re: Hello Mr. Fun and Games	12:07 AM	3.9 KB
Adrian Chen	question from a journalist	12:02 AM	3.94 KB
Luke Dashjr	Fun?	9/8/14	2.65 KB
Robert McMillan	← Re: New email account?	9/8/14	6.18 KB
Gregory Maxwell	Re: Hello Mr. Fun and Games	9/8/14	3.6 KB
Gregory Maxwell	← Hello Mr. Fun and Games	9/8/14	3.26 KB
Robert McMillan	← New email account?	9/8/14	4.67 KB
P2P Foundation	Kevin Parcell replied to your discussion "Bitcoin open source implem...	9/8/14	4.02 KB
P2P Foundation	Password Reset	9/8/14	3.24 KB
P2P Foundation	Hexlator replied to your discussion "Bitcoin open source implementat...	9/8/14	4 KB
sitelist-bounces@lists.sourceforge...	bitcoin-list subscription notification	9/8/14	4.45 KB
SourceForge Resources	Vectorization Gets Explicit with Intel's Updated Parallel Suite	9/8/14	12.67 KB
PitchBook PE & VC News	PitchBook News: Global PE and VC Fund Performance Update	9/8/14	154.87 KB
Mrs. Shriffa Abel	I am Mrs Sherifar Abell reply me urgently	9/8/14	4.04 KB
PYMNTS.com	The Big Innovation Disconnect | Apple Wallet At Disney Stores | Rak...	9/8/14	73.32 KB

1-50 of 11,659 e-mails Page 1 of 234

“Dear Satoshi. Your dox, passwords and IP addresses are being sold on the darknet. Apparently you didn’t configure Tor properly and your IP leaked when you used your email account sometime in 2010. You are not safe. You need to get out of where you are as soon as possible before these people harm you. Thank you for inventing Bitcoin.”

Olağan Şüpheliler

New Yorker – Michael Clear

http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis

Fast Company – Neal King and others

http://www.fastcompany.com/1785445/bitcoin-crypto-currency-mystery-reopened

Ted Nelson – Shinichi Mochizuki

http://www.theregister.co.uk/2013/05/19/ted_nelson_thinks_hes_outed_bitcoins_nakamoto/

News Week – Dorian Nakamoto

http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

Forbes – Hal Finney

http://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/#1c993b492639

New York Times – Nick Szabo

http://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html

Wired – Craig Wright

http://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/

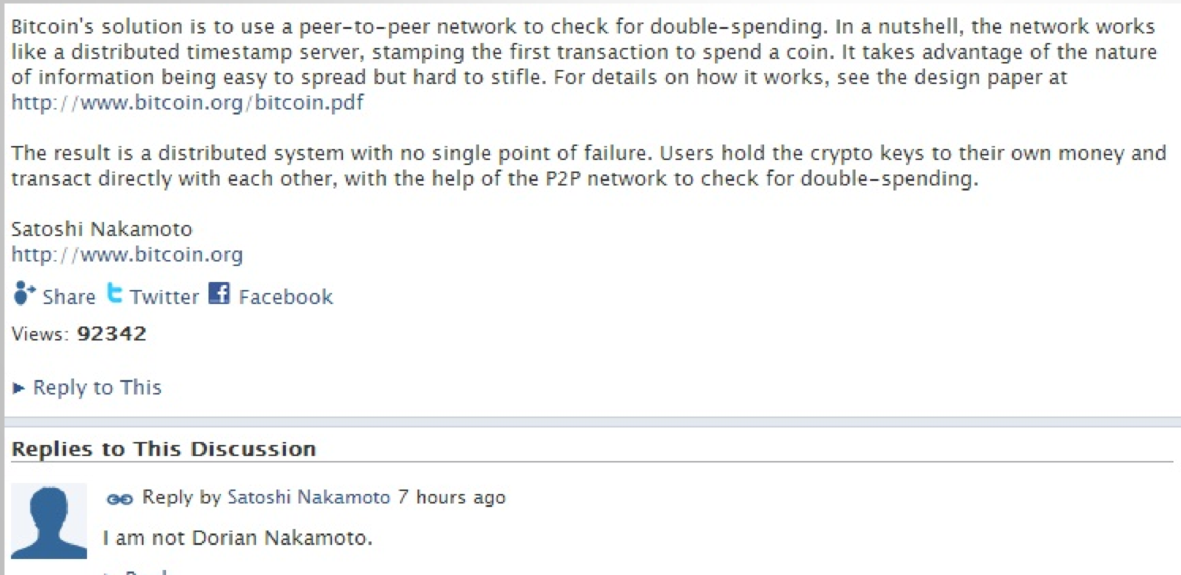
Olağan Şüpheliler, # Dorian Nakamoto

Newsweek
03.14.2014
BITCOIN'S FACE
THE MYSTERY MAN BEHIND THE CRYPTO-CURRENCY

6 Mart 2014, Leah McGrath Goodman

- Dorian Prentice Satoshi Nakamoto
- 65 yaşında
- Temple City, California sakini
- Savunma sanayii projelerinde sistem mühendisi, teknoloji ve finans şirketlerinde bilgisayar mühendisi...
- Japon kökenli Amerikan vatandaşı
- Hal Finney?'in bir kaç blok uzağında

? *"I am no longer involved in that and I cannot discuss it. It's been turned over to other people. They are in charge of it now. I no longer have any connection."* ?



Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at http://www.bitcoin.org/bitcoin.pdf

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

Satoshi Nakamoto
http://www.bitcoin.org

Share Twitter Facebook

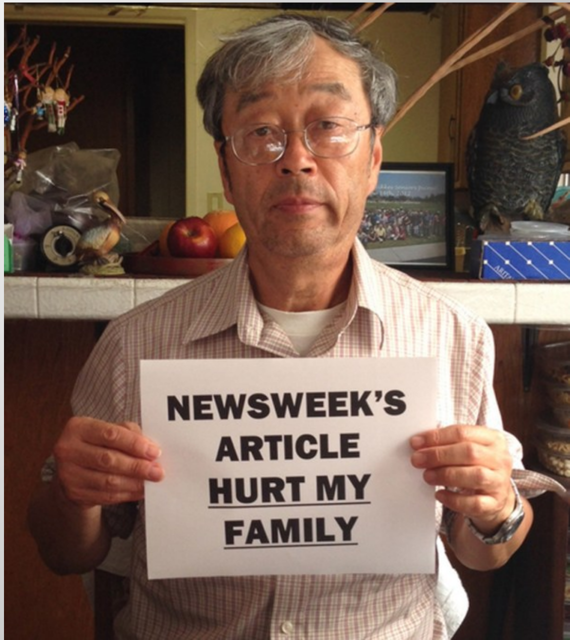
Views: 92342

► Reply to This

Replies to This Discussion

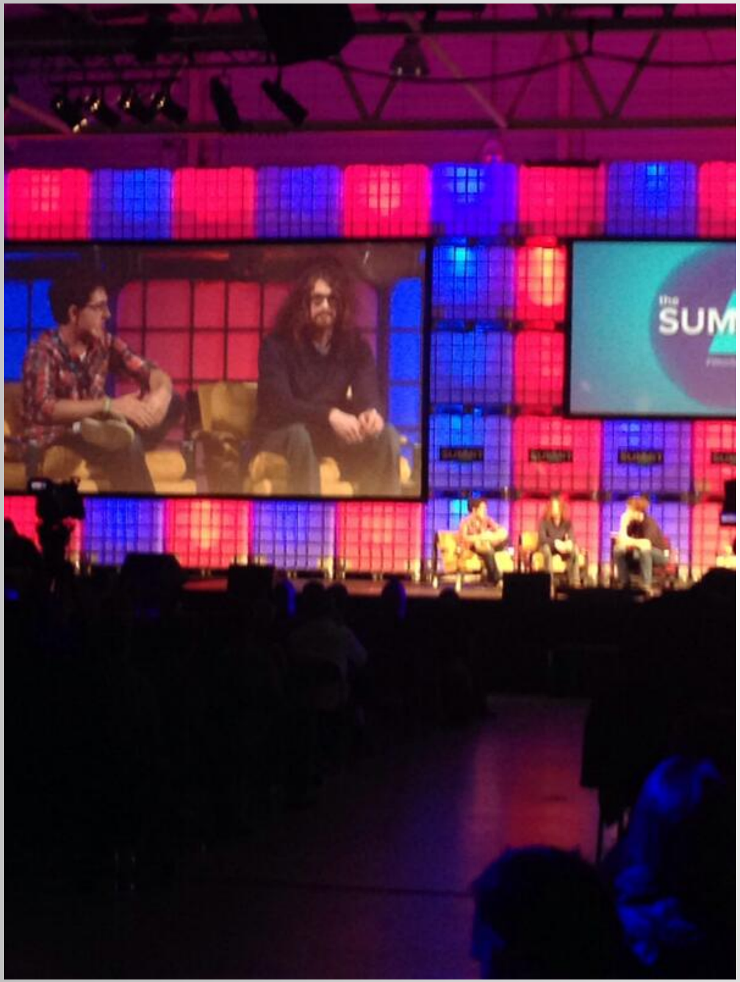
Reply by Satoshi Nakamoto 7 hours ago

I am not Dorian Nakamoto.



Olağan Şüpheliler, # 6, Michael Clear

TÜBİTAK



Business Insider dergisinde Joshua Davis imzalı makaleye göre:

- Crypto 2011 konferansında dikkat çeken
- Kriptografi konusunda İrlanda, Trinity Koleji'nde yüksek lisans mezunu
- İrlanda Bankalar Birliği tarafından para-ticaret yazılımı geliştirme amaçlı işe alınmış
- Ekonomi, kriptografi, eşten eşe (peer-to-peer) ağ teknolojisi konusunda son derece bilgili

BUSINESS INSIDER

"I'm not Satoshi, but even if I was I wouldn't tell you."
"You can't kill it, Bitcoin would survive a nuclear attack."

Olağan Şüpheliler, # 5, Jed McCaleb

- Tokyo merkezli bitcoin borsası Mt. Gox'un kurucusu
- eDonkey'in kurucularından,
- 2012'de Mt. Gox'u kurduktan 1-2 yıl sonra Ripple Laboratuvarlarının kurucularından
- Stellar'ın kurucusu

MT.GOX

ripple

STELLAR

- Japon kültürü hayranı
- Japonya'da ikamet

Mike Hearn - February 25, 2013, 12:48:54 PM

He communicated with a few of the core developers before leaving. He told myself and Gavin that he had moved on to other things and that the project was in good hands.

Olağan Şüpheliler, # 4, Dave Kleiman

- 1967 doğumlu
- Çocukluğundan itibaren teknoloji ve bilgisayar meraklısı
- 1986 helikopter teknisyeni
- 1990 bilgisayar suçları uzmanı
- 1995 motorsiklet kazası ve felçle birlikte artan bilgisayar merakı
- 40 – 50 karakterlik şifreler
- 2000'lerin başından itibaren metzdowd.com'daki E-posta listelerinde katkılar

- 2010 MRSA teşhisi (Metisilin Dirençli Stafilokok Aureus)
- 2008'de Bitcoin makalesinden aylar önce Gizmodo'ya iletilen bir mailde belgelenen Craig Wright bağlantısı

"I need your help editing a paper I am going to release later this year. I have been working on a new form of electronic money. Bit cash, Bitcoin..."
"You are always there for me Dave. I want you to be a part of it all."

- 2013 hastaneden çıkış
- 1 ay kadar sonra evde başından vurulmuş şekilde bulunma

Olağan Şüpheliler, # 4, Dave Kleiman

TÜBİTAK

- Gizmodo'ya gönderilen tamamlanmamış bir belgede Craig'in Kleiman'a emanet ettiği 1.1 milyon BTC…
- Ölümünden önce yanından ayırmadığı metal kasalı bir USB ve kız kardeşi IRA'ya miras…
- 14 Şubat'ta kız kardeş Ira'nın Craig Wright'a açtığı dava

"As reflected in the February 18, 2014 transcript, in the meeting, Craig's counsel states that the bitcoins W&K mined was held by Seychelles, Singapore, and UK trusts. As Dave owned between 50% to 100% of W&K, at least half of the bitcoins transferred to the trusts belonged to Dave."

Mahkemeye sunulan Mart 2014 tarihli Ira – Craig yazışması:

IRA : *"In one of the email exchanges between Dave and you, he mentioned that you had 1 million Bitcoins in the trust and since you said he has 300,000 as his part. I was figuring the other 700,000 is yours. Is that correct?,"*

Wright: *"Around that. Minus what was needed for the company's use,"*

Olağan Şüpheliler, # 3, Hal Finney

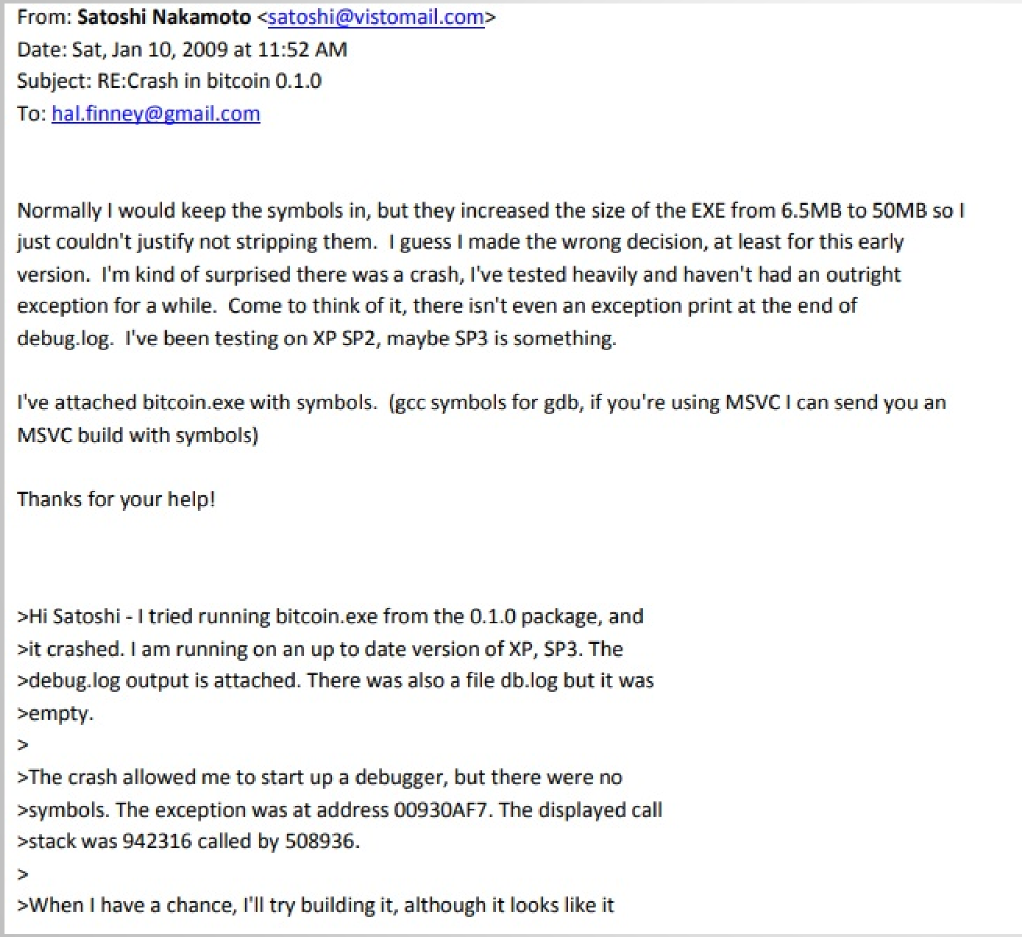
- d. 4 Mayıs 1956, ö. 28 Ağustos 2014
- İlk Bitcoin transferi yapılan kişi
- Lisans: California Institute of Technology, 1979
- PGP Corporation'da Phil Zimmermann'dan sonra işe alınan 2. geliştirici
- 2011, Emeklilik
- 1990'larda, Kriptografik aktivist
- Cypherpunks hareketinin içinde
- 2004'te ilk yeniden kullanılabilir PoW sistemi

"The computer can be used as a tool to liberate and protect people, rather than to control them."

- Ekim 2009'da, kendisine Ağustos 2009'da ALS (Amyotrophic Lateral Sclerosis) teşhisi konulduğunu açıkladı

Olağan Şüpheliler, # 3, Hal Finney

- 20,000 kelimeye göre Stilometri analizinde Satoshi’nin diline en yakın aday (Juola & Associates Yazım Danışmanlık Firması)



From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sat, Jan 10, 2009 at 11:52 AM
Subject: RE:Crash in bitcoin 0.1.0
To: hal.finney@gmail.com

Normally I would keep the symbols in, but they increased the size of the EXE from 6.5MB to 50MB so I just couldn't justify not stripping them. I guess I made the wrong decision, at least for this early version. I'm kind of surprised there was a crash, I've tested heavily and haven't had an outright exception for a while. Come to think of it, there isn't even an exception print at the end of debug.log. I've been testing on XP SP2, maybe SP3 is something.

I've attached bitcoin.exe with symbols. (gcc symbols for gdb, if you're using MSVC I can send you an MSVC build with symbols)

Thanks for your help!

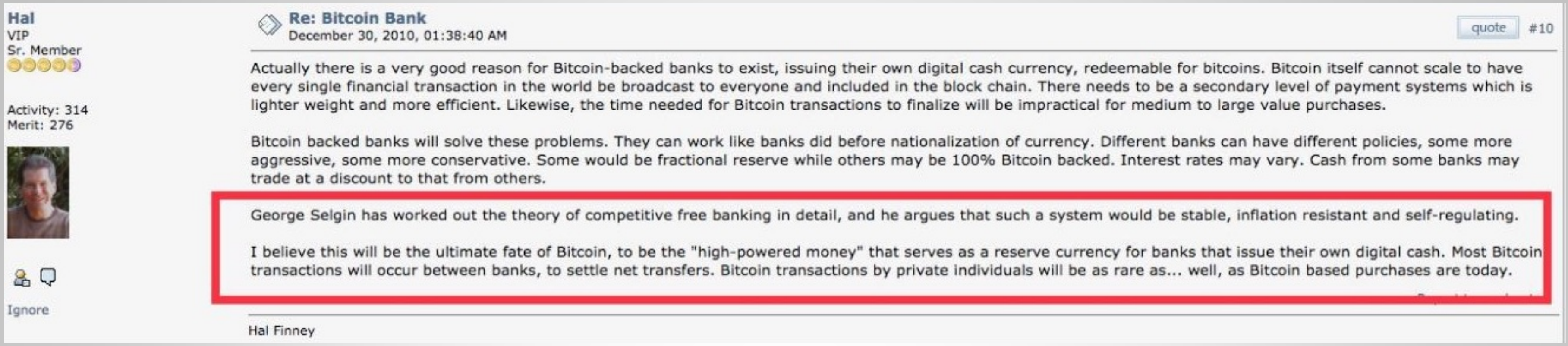
\>Hi Satoshi - I tried running bitcoin.exe from the 0.1.0 package, and
\>it crashed. I am running on an up to date version of XP, SP3. The
\>debug.log output is attached. There was also a file db.log but it was
\>empty.
>
\>The crash allowed me to start up a debugger, but there were no
\>symbols. The exception was at address 00930AF7. The displayed call
\>stack was 942316 called by 508936.
>
\>When I have a chance, I'll try building it, although it looks like it

- 2014’te Hal, Satoshi ile olan ve Bitcoin yazılımının v0.1.0’dan v0.13’e geçişine dair yazışmaları Wall Street Journal ile paylaştı.

- Yazışmalar 10 Ocak ve 24 Ocak 2009 tarihleri arasındaydı

- 12 Ocak 2009’da 170. blokta Hal 10BTC’lik ilk transferi aldı

Olağan Şüpheliler, # 3, Hal Finney



Hal
VIP
Sr. Member

Activity: 314
Merit: 276

Ignore

Re: Bitcoin Bank
December 30, 2010, 01:38:40 AM

quote #10

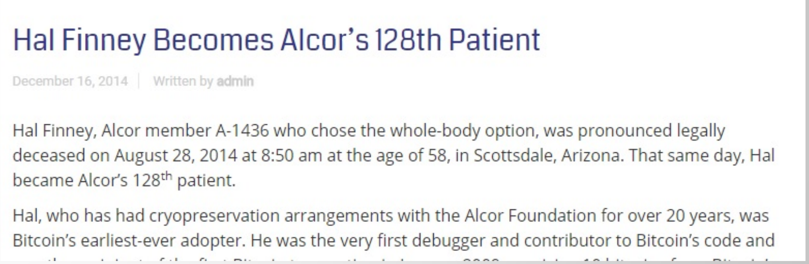
Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases.

Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

George Selgin has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating.

I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.

Hal Finney



Hal Finney Becomes Alcor's 128th Patient

December 16, 2014 | Written by admin

Hal Finney, Alcor member A-1436 who chose the whole-body option, was pronounced legally deceased on August 28, 2014 at 8:50 am at the age of 58, in Scottsdale, Arizona. That same day, Hal became Alcor's 128th patient.

Hal, who has had cryopreservation arrangements with the Alcor Foundation for over 20 years, was Bitcoin's earliest-ever adopter. He was the very first debugger and contributor to Bitcoin's code and

- 28 Ağustos 2014'te ölümünden sonra Hal'ın vücudu, Alcor Cryonics'te dondurularak saklanmaya başladı.
- Alcor'a ödeme Bitcoin ile yapıldı …

Olağan Şüpheliler, # 2, Nick Szabo

TÜBİTAK

- 1989, University of Washington, Bilgisayar Bilimleri mezunu
- Bilgisayar bilimcisi, yazar ve George Washington Üniversitesi hukuk profesörü
- 1990'ların başında 6 ay boyunca DigiCash'te danışman olarak çalıştı
- 1994, Akıllı konrat kavramı
- 1998, Bit Gold → Bitcoin mimarisine ön adım

Bit Gold fikrini Hal Finney ve Wei Dai'nin de içinde olduğu bir grupla paylaştı. ***Hal Finney Bit Gold'un çalışan bir versiyonunu ortaya çıkarmak için çalıştı***

- Yazma stili
  2014'te Aston Üniversitesi'nde araştırmacılar → Satoshi ile yazma stili uyumunun sıradışılığı
- Bitcoin makalesinde Bit Gold'la sıradışı benzerlikler olmasına rağmen, Bit Gold'a referans yok
- 2008 baharında kendi bloğundan Bit Gold fikrini paylaştı ve bu fikri hayata geçirecek programcı arayışını belirtti
  Web arşivleri bu bildirimin tarihinin Bitcoin'in ortaya çıkışı sonrasında değiştirildiğini göstermektedir.
- Bitcoin çıktığı sene Nick Sessizliğe bürünmüştü
- Bitcoin'in 1c bariyerini kırıp 20c'e çıktığı 2010'da Nick yine sessizdi
- Nick Satoshi'nin kendi projesinden çekildiği 2010'dan sonra 2011'de Bitcoin'le ilgili konuşmaya başladı
- 10 sene boyunca kriptopara konusunda çalışma geçmişi, Bitcoin konusundaki gelişmeler konusunda hiç şaşırmıyor olması
- 15 Mayıs 2015, Nathaniel Popper, New York Times

Olağan Şüpheliler, # 1, Craig Wright

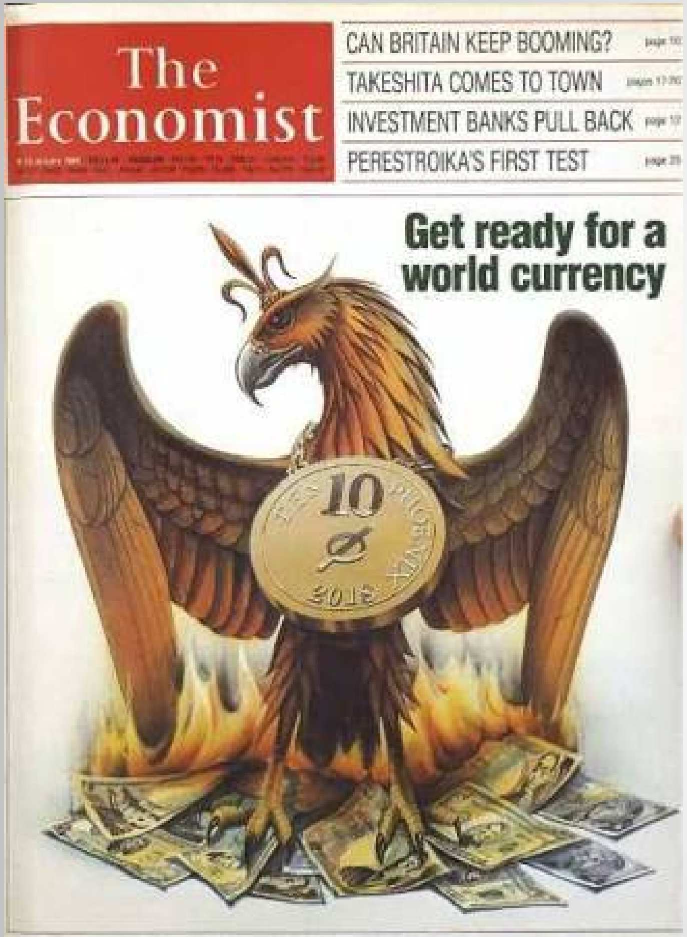
- Kasım 1970 doğumlu, Avustralyalı bilgisayar bilimcisi ve işadamı,
- Dünyanın ilk online casino'sunun yazılım mimarı…

"I was the main part of it, but other people helped me,"

- Aralık 2015'te Wired ve Gizmodo teknoloji dergileri yayınladıkları raporda Craig Wright'ı Bitcoin'in kurucusu olarak gösterdi
  - 2008 yılında Dr Wright kriptopara ile ilgili bir makale yayınlamak istediği 2008'de blokundan açıklamış
  - Avustralya saati ile 10 Ocak 2009'daki bir paylaşımında ise Bitcoin'in bir gün sonraki doğuşunu ilan etmişti. Bu Amerika saat diliminde Bitcoin'in ilk açık kaynak kodlu istemci kodunun paylaşıldığı 9 Ocak 2009, 15.00'ten önceki bir zamandı
- Haberin ortaya çıkmasından saatler sonra Avustralya polisi Wright'ın evine baskın düzenledi (ATO)

"We have lawyers negotiating with them over how much I have to pay,"

Olağan Şüpheliler, # 1, Craig Wright


The Economist
CAN BRITAIN KEEP BOOMING?
TAKESHITA COMES TO TOWN
INVESTMENT BANKS PULL BACK
PERESTROIKA'S FIRST TEST
Get ready for a world currency
10
PHOENIX
2018

- 2 Mayıs 2016'da **Economist**, BBC ve GQ Magazin'e yaptığı açıklamalarda Bitcoin'in kurucusu olduğunu ilan etti

Bitcoin Vakfı'nın şef mühendisi olan Gavin Andersen Wright'ın açıklamalarına inandığını ve Londra'da biraraya gelmelerinden sonra Wright'ın bitcon'in arkasındaki isim olduğuna ikna olduğunu belirtti...

- Bitcoin Vakfı'nın kurucularından Jon Matonis, Wright'ın bir mesajı Blok1 ve Blok 9'da Satoshi'nin kullanmış olduğu gizli anahtarlarla imzalayıp doğrulayabildiğini açıkladı. Gavin Andresen de bu işlemin sadece Satoshi'nin sahip olabileceği anahtarlarla yapılabileceğini doğruladığını bildirdi…

Olağan Şüpheliler, # 1, Craig Wright

TÜBİTAK

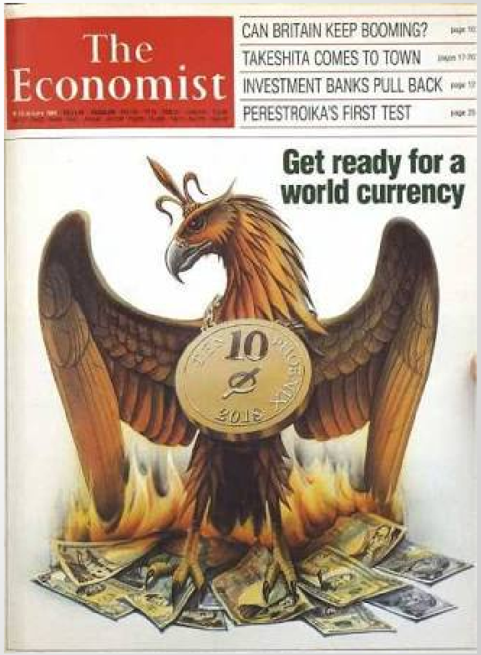
- 6 Mayıs 2016’da Andresen’in Bitcoin core kodları üzerinde değişiklik yapma hakkı alındı.

- Wright, Nakomoto ismini 17. yüzyılda yaşamış Japon filozof ve ticaret adamı Tominaga Nakamoto’dan esinlenerek seçtiğini belirtti

  Mukishinron → Ateizmin Japon versiyonu

  Budizm, Konfüçyüsçüizm ve Şintoizm üzerine çalışmaları olan…

‘So that’s where you say you got the Nakamoto part?’ I asked. ‘From the 18th-century iconoclast who criticised all the beliefs of his time?’ ‘Yes.’ ‘What about Satoshi?’ ‘It means “ash”,’ he said. ‘The philosophy of Nakamoto is the neutral central path in trade. Our current system needs to be burned down and remade. That is what cryptocurrency does – it is the phoenix …’ ‘So satoshi is the ***ash from which the phoenix*** *…’ ‘Yes. And Ash is also the name of a silly Pokémon character. The guy with Pikachu.’* ***Wright smiled****. ‘In Japan the name of Ash is Satoshi,’ he said. ‘So, basically, you named the father of bitcoin after Pikachu’s chum?’ ‘Yes,’ he said. ‘That’ll annoy the buggery out of a few people.’ This was something he often said, as if annoying people was an art.*


The Economist
CAN BRITAIN KEEP BOOMING?
TAKESHITA COMES TO TOWN
INVESTMENT BANKS PULL BACK
PERESTROIKA'S FIRST TEST
Get ready for a world currency
10
2018

9 Ocak 1988,
Phoenix,
Tek Dünya Parasına Hazır olun

Olağan Şüpheliler, # 0, Nakamoto SAtoshi

Department of Defence, USA

- DIA(Defence Intelligence Agency)
- **NSA (National Security Agency)**
- NGA (National Geospatial-Intelligence Agency)
- NRO (National Reconnaissance Office)
- **DARPA (Defense Advanced Research Projects Agency)** → The Tor project (the anonymous online network)

1996, NSA makalesi “*How To Make A Mint: The Cryptography of Anonymous Electronic Cash*”

Tatsuaki ***Okamoto***, NSA Kriptoloji Bölümü

Okamoto,“*An Efficient Divisible Electronic Cash Scheme*“

Elektronik paranın bir bankadan veya merkezi bir kurumdan çekileceği öngörüsü…

“a scheme that merely allows people to prove their balances in banks and sign their transfers, of a centralized currency where the main service nodes (banks) have the final authority of whatever can happen”

1997, Adam Back, Proof of Work (hashcash) tanımı

Olağan Şüpheliler, # 0, Nakamoto SAtotoshi

CONTENTS
INTRODUCTION
1. WHAT IS ELECTRONIC CASH?
1.1 Electronic Payment
1.2 Security of Electronic Payments
1.3 Electronic Cash
1.4 Multiple Spending
2. A CRYPTOGRAPHIC DESCRIPTION
2.1 Public-Key Cryptographic Tools
2.2 A Simplified Electronic Cash Protocol
2.3 Untraceable Electronic Payments
2.4 A Basic Electronic Cash Protocol
3. PROPOSED OFF-LINE IMPLEMENTATIONS
3.1 Including Identifying Information
3.2 Authentication and Signature Techniques
3.3 Summary of Proposed Implementations
4. OPTIONAL FEATURES OF OFF-LINE CASH
4. 1 Transferability
4.2 Divisibility
5. SECURITY ISSUES
5.1 Multiple Spending Prevention
5.2 Wallet Observers
5.3 Security Failures
5.4 Restoring Traceability
CONCLUSION
REFERENCES

REFERENCES

1. Stefan Brands, *Untraceable Off-Line Cash in Wallets with Observers*, Advances in Cryptology CRYPTO '93, Springer-Verlag, pp. 302-318.
2. David Chaum, *Achieving Electronic Privacy*, Scientific American (August 1992), 96-101.
3. David Chaum, *Security without Identification: Transaction Systems to make Big Brother Obsolete*, ACM 28 no. 10 (Oct 1985), 1030-1044.
4. David Chaum, Amos Fiat, and Moni Naor, *Untraceable Electronic Cash*, Advances in Cryptology CRYPTO '88, Springer-Verlag, pp. 319-327.
5. David Chaum and Torben Pedersen, *Transferred Cash Grows in Size*, Advances in Cryptology - EUROCRYPT '92, Springer-Verlag, pp. 390-407.
6. David Chaum and Torben Pedersen, *Wallet Databases with Observers*, Advances in Cryptology CRYPTO '92, Springer-Verlag, pp. 89-105.
7. Tony Eng and Tatsuaki Okamoto, *Single-Term Divisible Electronic Coins*, Advances in Cryptology EUROCRYPT '94, Springer-Verlag, pp. 311-323.
8. Niels Ferguson, *Extensions of Single-term Coins*, Advances in Cryptology - CRYPTO '93, Springer-Verlag, pp. 292-301.
9. Niels Ferguson, *Single Term Off-Line Coins*, Advances in Cryptology - EUROCRYPT '93, Springer-Verlag, pp. 318-328.
10. Alfred J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, 1993.
11. Tatsuaki Okamoto, *An Efficient Divisible Electronic Cash Scheme*, Advances in Cryptology - CRYPTO '95, Springer-Verlag, pp. 438-451.
12. Tatsuaki Okamoto and Kazuo Ohta, *Universal Electronic Cash*, Advances in Cryptology - CRYPTO '91, Springer-Verlag, pp. 324-337.
13. Sebastiaan von Solms and David Naccache, *On Blind Signatures and Perfect Crimes*, Computers & Security 11 (1992), 581-583.
14. Markus Stadler, Jean-Marc Piveteau, and Jan Camenisch, *Fair Blind Signatures*, Advances in Cryptology - EUROCRYPT '95, Springer-Verlag, pp. 209-219.

Olağan Şüpheliler, # 0, Nakamoto SAtoshi

1. Kaoru Kurosawa, **Satoshi Obana**, Combinatorial Bounds on Authentication Codes with Arbitration, Designs, Codes and Cryptography, Volume 22(3), pp. 265 - 281, Springer, 2001.

2. **Satoshi Obana**, Kaoru Kurosawa, Bounds and Combinatorial Structure of Multi-Receiver-Codes, Designs, Codes and Cryptography, Volume 22(1), pp. 47 - 63, Springer, 2001.

3. **Satoshi Obana**, Kaoru Kurosawa, Combinatorial Classification of Optimal Authentication Codes with Arbitration, Designs, Codes and Cryptography, Volume 20(3), pp. 281 - 305, Springer, 2000.

Clear thinking inside the foundation

+

?
=

Satoshi Obana

Tatsuaki **Okamoto**

http://academic.research.microsoft.com/Author/1002804/tatsuaki-okamoto
Fields: Security & Privacy, Electrical & Electronic Engineering, Algorithms & Theory

Satoshi Nakamoto
Nakamoto SAtoshi

Olağan Şüpheliler, # 0, Nakamoto SAtoshi

“In-Q-Tel… is a not-for-profit venture capital firm that invests in high-tech companies for the sole purpose of keeping the Central Intelligence Agency, and other intelligence agencies, equipped with the latest in information technology in support of United States intelligence capability”

- 2005, In-Q-Tel 5000 Google hisse senedi sattı
- 2006, eski CIA çalışanı Robert David Steele, Google’ın CIA, In-Q-Tel ve NSA’ten para aldığını açıkladı
- 2010, Google elektronik varlıklarının güvenliğini sağlamak için doğrudan NSA’le çalıştığını açıkladı

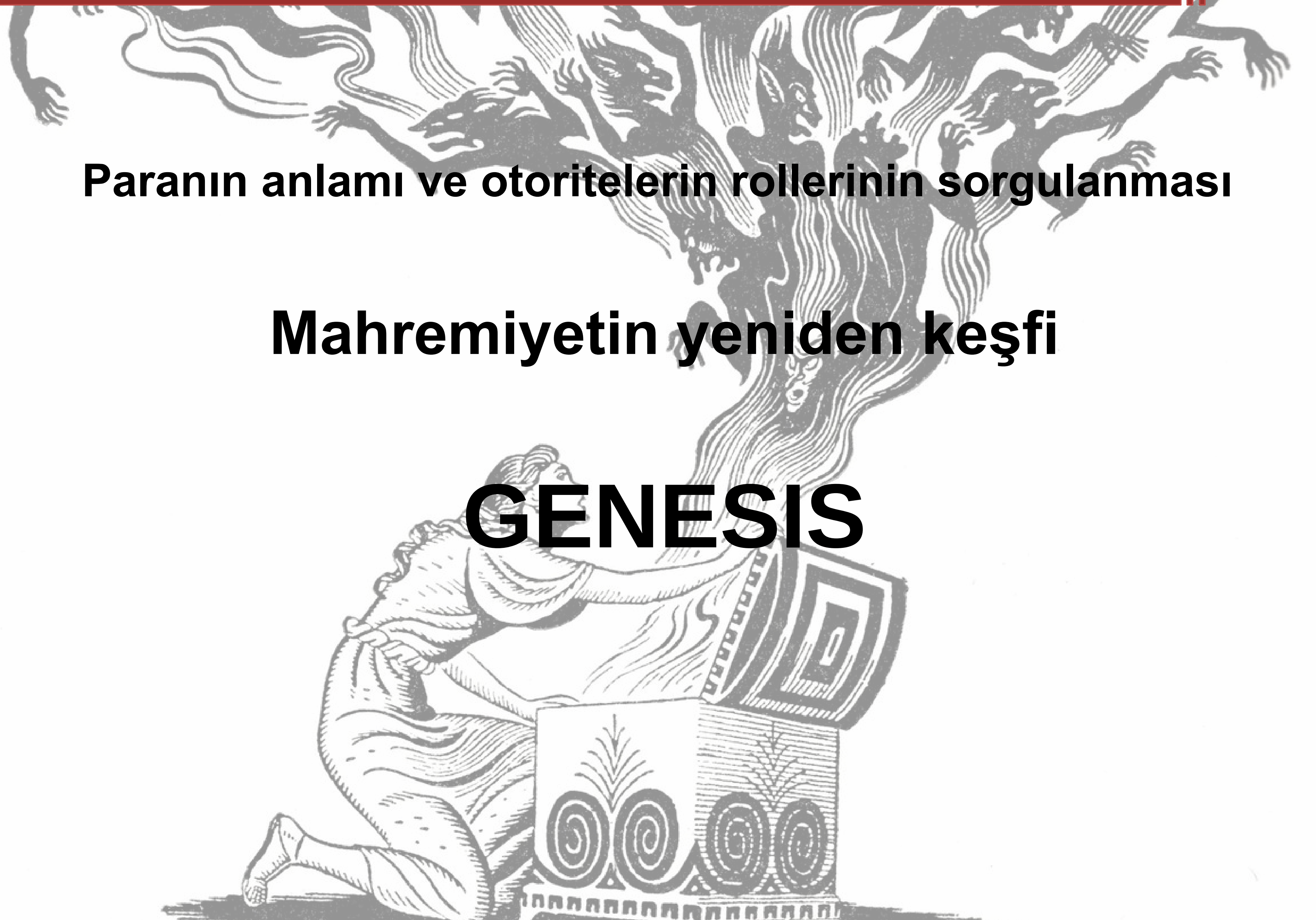
Özet

NEWSWEEK'S
ARTICLE
HURT MY
FAMILY

moni
makes the world
go round.

ADVOCACY
ECTION OF

Pandora’nın Kutusu



Paranın anlamı ve otoritelerin rollerinin sorgulanması

Mahremiyetin yeniden keşfi

GENESIS