Frontiers in Blockchain Research

Course Introduction

Class 01

Jan 13, 2026

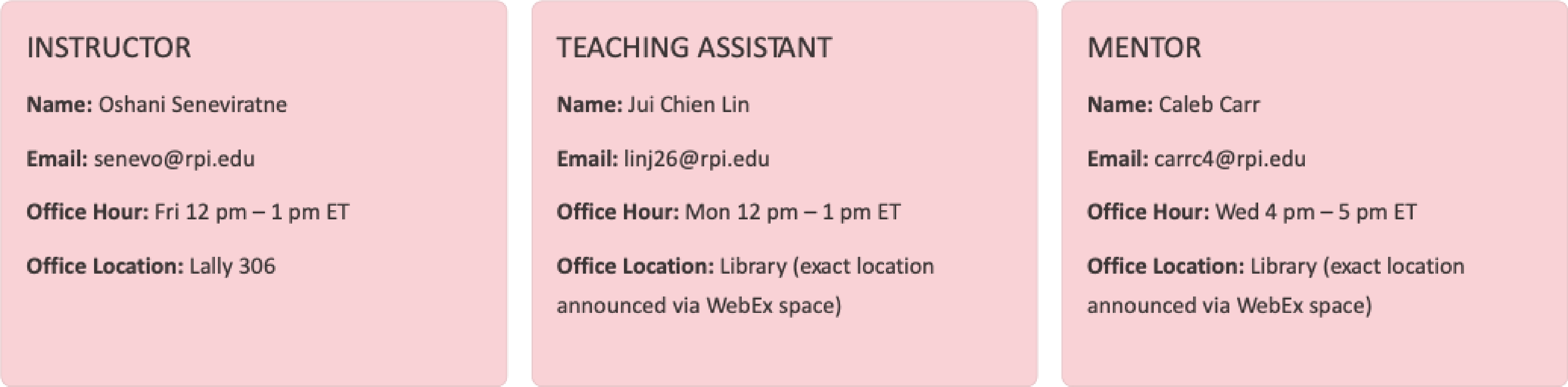
Oshani Seneviratne

Assistant Professor

Department of Computer Science

Rensselaer Polytechnic Institute, Troy NY USA

Course Team



INSTRUCTOR

Name: Oshani Seneviratne

Email: senevo@rpi.edu

Office Hour: Fri 12 pm – 1 pm ET

Office Location: Lally 306

TEACHING ASSISTANT

Name: Jui Chien Lin

Email: linj26@rpi.edu

Office Hour: Mon 12 pm – 1 pm ET

Office Location: Library (exact location announced via WebEx space)

MENTOR

Name: Caleb Carr

Email: carrc4@rpi.edu

Office Hour: Wed 4 pm – 5 pm ET

Office Location: Library (exact location announced via WebEx space)

Class Logistics

- **Prerequisites:**
  - A big interest in learning the SoTA blockchain research.
- **Other Preferred Requirements:**
  - CSCI 2300 (Introduction to Algorithms)
  - CSCI 2600 (Principles of Software)
  - CSCI 4100 (Machine Learning from Data) or CSCI 4150 (Introduction to Artificial Intelligence) or familiarity with basic machine learning algorithms
  - CSCI 4230 (Cryptography and Network Security I) or familiarity with basic cryptography
  - CSCI 4510 (Distributed Systems and Algorithms)
- **Room Location:** J-ROWL 1W01
- **Time:** Tue/Fri 2:00pm - 3:50pm ET
- **Course Website:** https://cs.rpi.edu/academics/courses/spring26/csci4962
  - Lecture material are posted here
- **Submitty:** https://submitty.cs.rpi.edu/courses/s26/csci4962
- **WebEx Space:** "Frontiers in Blockchain Research - Spring 2026"
  - https://eurl.io/#-gJShBLpd (please use your rpi.edu email address to join)

Course Assessment & Grading

4000 Level

- Paper Presentations: 20%
- Class Participation: 10%
- In-Class Quizzes: 30%
- Project: 40%
- Paper: optional (strongly encouraged)

6000 Level

- Paper Presentations: 20%
- Class Participation: 10%
- In-Class Quizzes: 20%
- Project: 30%
- Paper: 20%

Students taking a 6000-level course, regardless of student status (i.e., Undergraduate or Graduate), must satisfy the learning outcomes at the 6000 level if they expect to receive graduate credit for the course.

Grade – letter scale:

93% + is an A; 90%-92% is an A-; 87%-89% is a B+; 83%-86% is a B; 80%-82% is a B-; 77%-79% is a C+; 73%-76% is a C; 70%-72% is a C-; 65%-69% is a *D+; 60%-64% is a *D; 0%-59% is an F.

*Note: Students taking the course at the 6000 level cannot receive a D+/D grade.

Quick Introductions

- Name
- Major
- Level (4000/6000)
- Why are you interested in this course?

Course Goals/Objectives

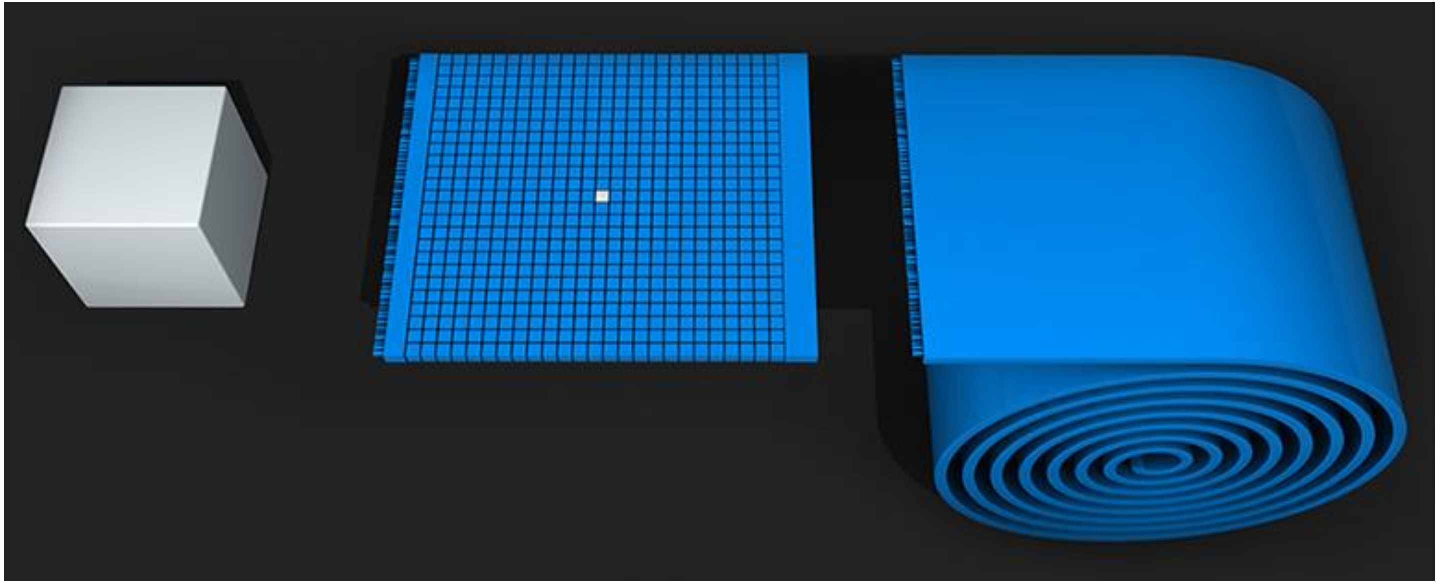
- Understand foundational blockchain principles
- Critically evaluate blockchain protocols and architectures
- Assess security, privacy, and cryptographic guarantees
- Examine programmability and smart contract systems
- Analyze economic, governance, and socio-technical dimensions
- Engage with cutting-edge research and open problems
- Develop independent research skills
- Bridge theory and practice

Learning Outcomes

- **Foundations:** Explain the core principles of blockchain systems and how they relate to seminal research.
- **Protocol Analysis:** Compare and evaluate major blockchain architectures (PoW, PoS, BFT-style consensus, Layer-2 scaling) using clear criteria such as security, scalability, decentralization, and real-world constraints.
- **Security & Privacy Reasoning:** Assess security threats and privacy mechanisms in blockchain systems (e.g., smart contract vulnerabilities, incentive attacks, ZK proofs/formal methods) and argue about trade-offs and mitigations.
- **Research Literacy & Communication:** Critically read and synthesize blockchain research papers, leading scholarly discussions and communicating technical insights effectively in presentations and written critiques.
- **[6000 level] Research Paper Writing:** Develop a publication-style research artifact (e.g., a workshop-ready paper, short research paper, or structured research proposal) that identifies a gap in the literature, motivates a contribution, and presents a coherent methodology and evaluation plan grounded in prior work.

Blockchain Building Blocks

The Parts



THE RECORD
Can contain anything

THE BLOCK
A bundle of records

THE CHAIN
All the blocks linked together

Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

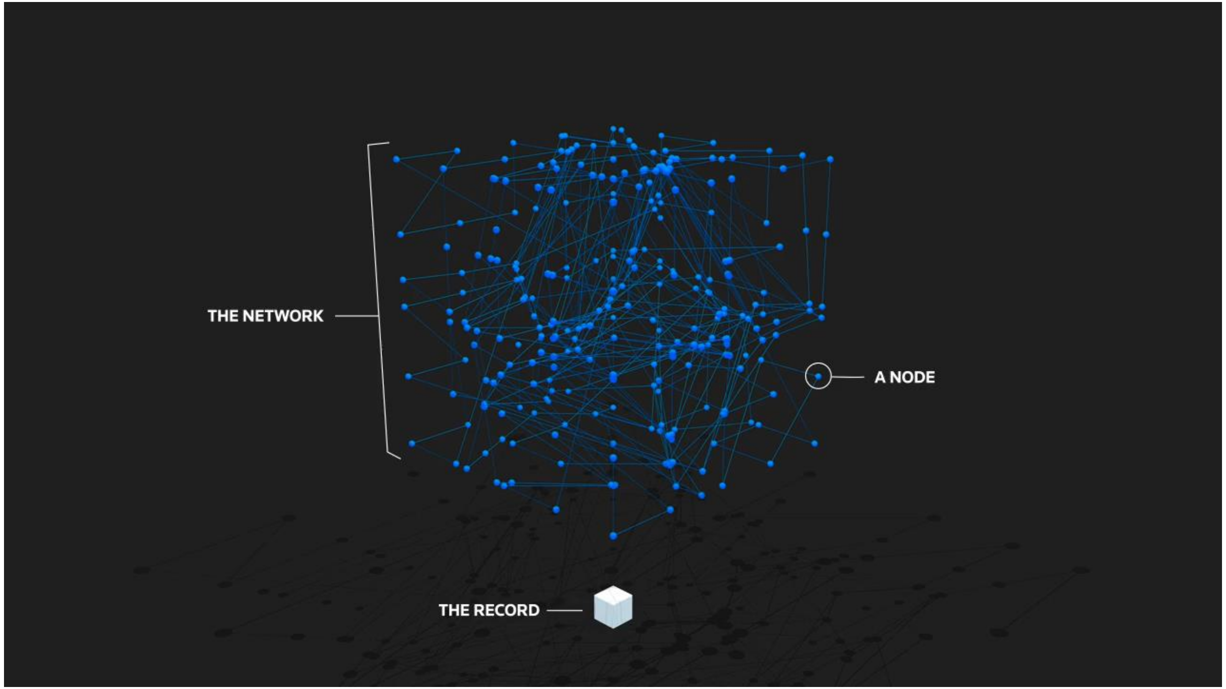
RPI

Step 1: Transaction

Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

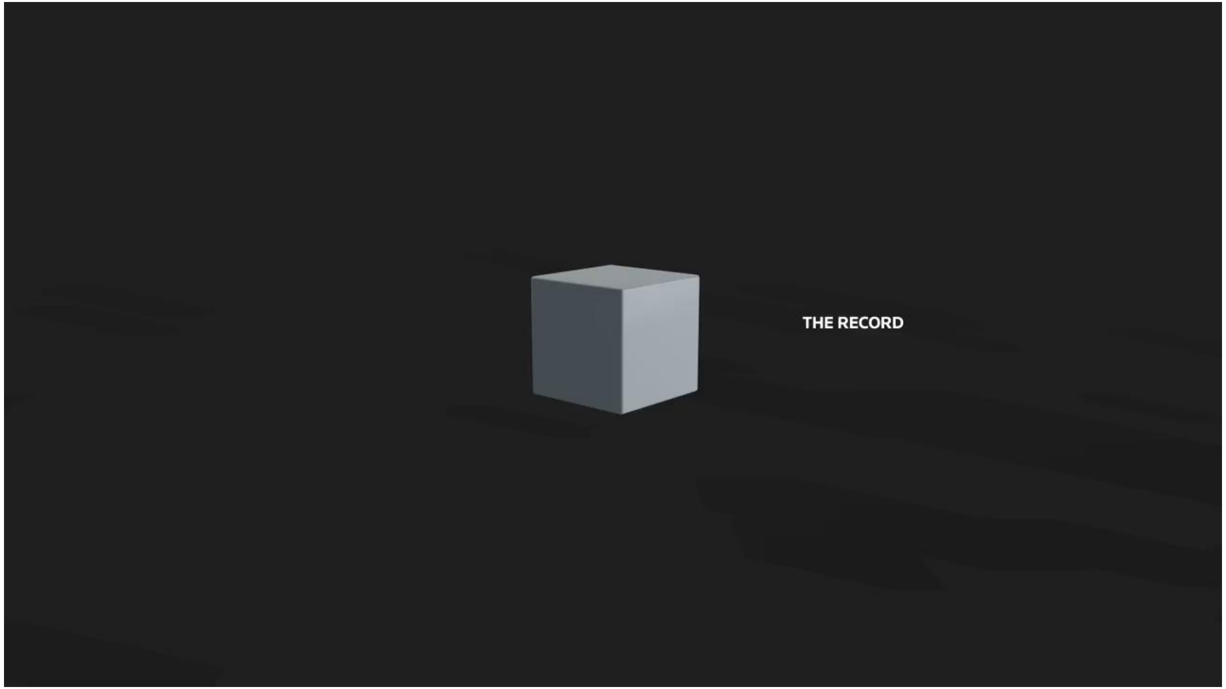
RPI

Step 2: Distributed Consensus



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

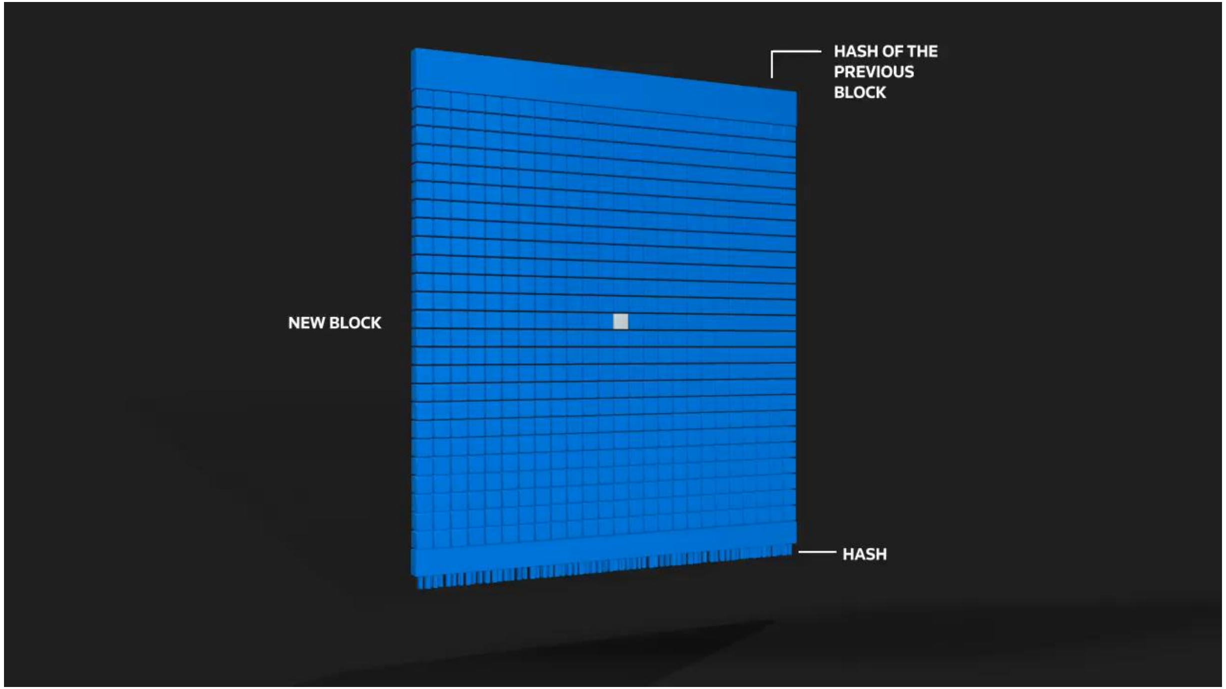
Step 3: Block Creation



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

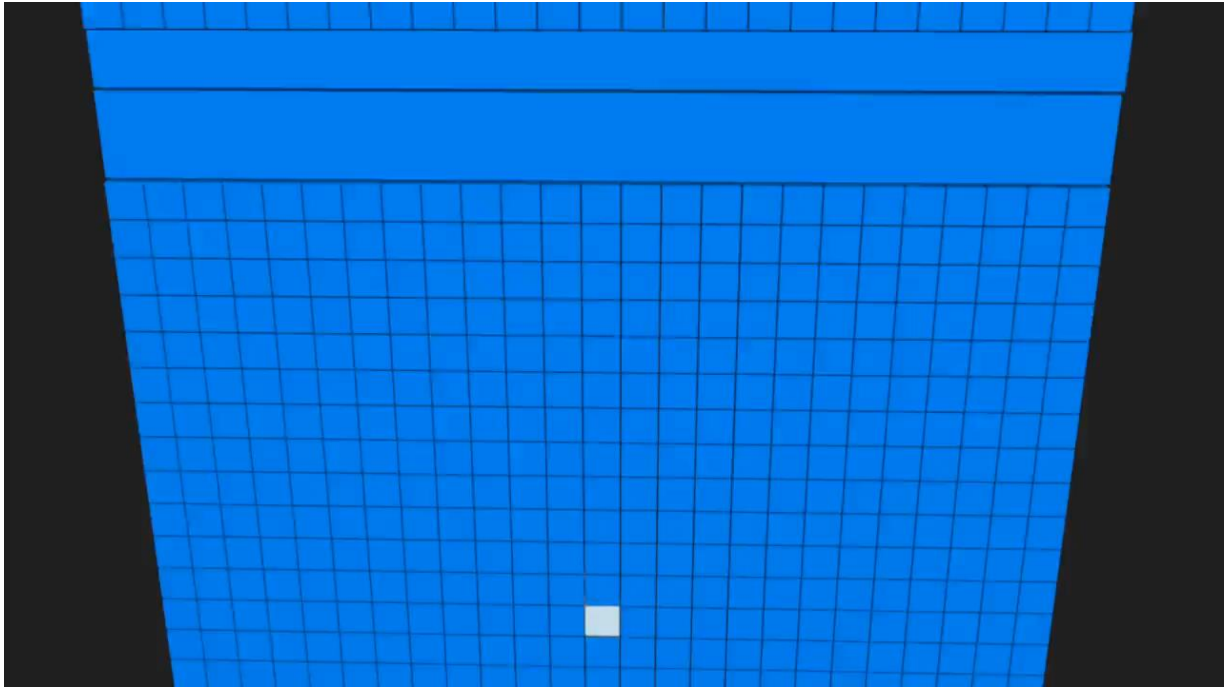
RPI

Step 4: Adding the block to the blockchain



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

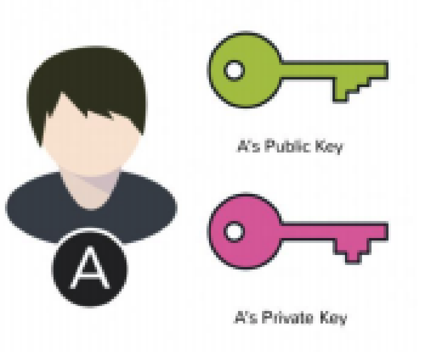
A Transaction in a committed block is difficult to change



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

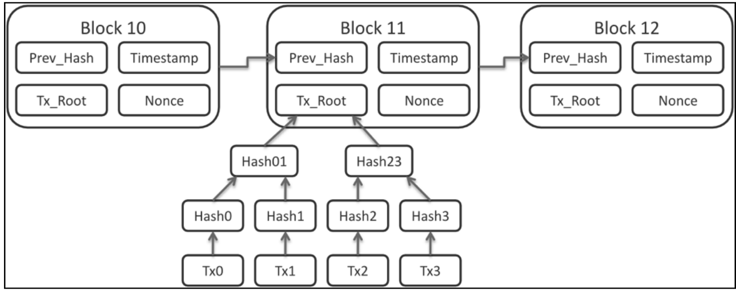
Blockchain != Cryptocurrency

- Cryptocurrency is an application that sits on top of a blockchain.
- **This course is not about cryptocurrencies!**
- We analyze technologies like the following and how they interface with AI.
- However, we should learn from the success of the most prominent (and successful blockchain application, i.e., cryptocurrencies.



Cryptographic Hashes and Identities

Consensus Protocol



Ledger aka "Chain"

Blockchain Pillars

- **Authenticity (cryptographic)**: creates transactions that are impervious to fraud through the use of digital signatures, establishing a shared truth
- **Shared**: the more entities participating in the blockchain, the more value it brings
- **Distributed**: many replicas of the blockchain database, making it more fault-tolerant
- **Ledger**: read/write once database maintaining an immutable record of every transaction

Blockchain Hype?

- Blockchains are largely based on **well-established** and **understood** technologies:
    - cryptography,
    - distributed databases and networks,
    - peer-to-peer,
    - discovery and network protocols, etc.
- It’s the **composite** of these technologies that creates a big impact and disruption across all industries (starting in financial services)
- Initial designs (**bitcoin**) proved to be **resilient**.
- **Smart contracts** showed the real potential for blockchain in **securely transferring value** and creating future **binding contracts** in a **trustless environment.**

Disruptive Effect of Blockchain

- Removing middleman processes makes things more efficient and cost-effective
- Peer-to-peer value exchange reduces centralized control
- One ledger instead of comparing multiple ledgers
- More collaborative economy – shared costs, risks, etc.
- Dramatic changes in how identity is defined and controlled

Why study blockchain? Why now?

- Blockchain technology has:
  - created an industry worth trillions of dollars
  - launched a wave of innovation in distributed systems, cryptography, privacy, security, and economics
- Two views:
  - Some believe that blockchains will be **integral to the future of money, governments, and the Internet**.
  - Others claim that this is a **transient bubble** and cryptocurrencies will be relegated to a footnote in history.

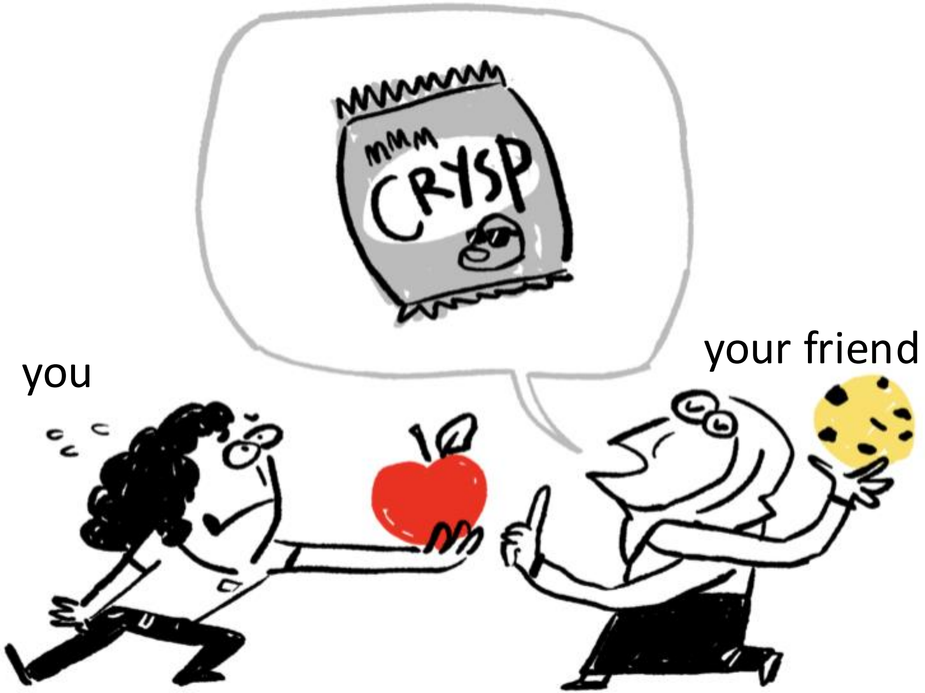
Minting money out of thin air?

- To create a free-floating digital currency that is likely to acquire real value, you need to have something that’s **scarce by design** (gold or diamonds)
- In the digital realm, one way to achieve scarcity is to design the system so that minting money requires **solving a computational problem** (or “puzzle”) that takes a while to crack
- This idea has been around since the early 90’s: first to solve email spam (**Hashcash**)
  - To enforce this requirement, the recipient’s email program would simply ignore your email if you didn’t attach the solution to the computational puzzle.
  - For the average user, it wouldn’t be that much of a barrier to sending emails because you’re not sending emails very frequently.
  - But if you’re a spammer, you’re trying to send out thousands or millions of emails all at once, and solving those computational puzzles could become prohibitive!

What is Money? An Artist’s Make and Take

https://www.wsj.com/video/what-is-money-an-artists-make-and-take/DAC445B2-B01C-42ED-B928-91E5E7FC3BA3.html

Exchanging Goods and Services: Bartering



Is it possible for both you and your friend to get what you want by bartering?

A. No, it's not possible to give up your apple to receive the cookie.
B. Only if your friend is willing to compromise.
[✓ C. Yes, but it requires a third person with different snacks and preferences.]

What is the role of money?

If your friend thinks that trading you her cookie in exchange for one dollar is a good deal for her, what is she assuming?

A. The cookie is worth exactly one dollar to her — no more, no less.

[✓ B. She'll be able to use the dollar to buy something else she wants later.]

C. The paper bill can directly meet her wants and needs.

D. All of the above

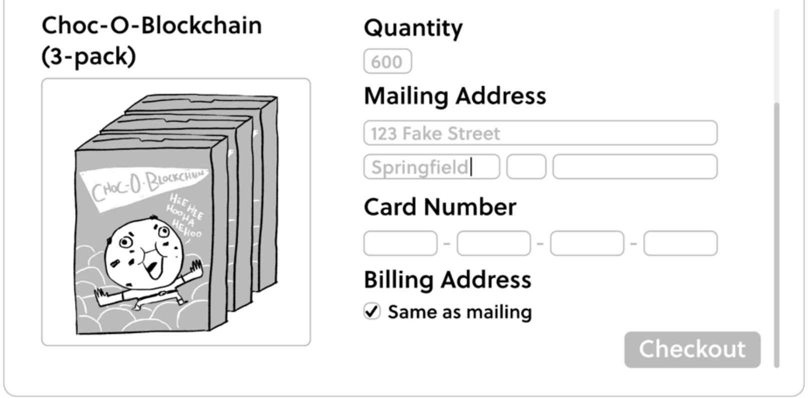
Precious Metals (or "Gold 1.0") as Money

- They don't degrade over time.
- They're rare enough that it takes a lot of work to find more.
- They're common enough that it's possible to find more.
- The amounts that most people would have are easy to carry around.
- Precious metals don't meet a basic need.

Source: https://spectrum.ieee.org/at-work/innovation/a-brief-history-of-money

Credit

- You don’t even need to trade gold coins or pieces of fancy paper (i.e., cash) for goods, you also have the option to trade a **promise** that you’ll pay the person back later.
- Why might someone be hesitant to accept credit as payment rather than cash?
- What is one downside to using credit cards when shopping online?
  - A. You need to have a lot of cash on hand to use a credit card
  - B. [✓ You have to share your credit card number.]
  - C. It takes a long time for your payment info to go through.
  - D. There are no downsides



Choc-O-Blockchain (3-pack)

Quantity
600

Mailing Address
123 Fake Street
Springfield

Card Number
- - -

Billing Address
✓ Same as mailing

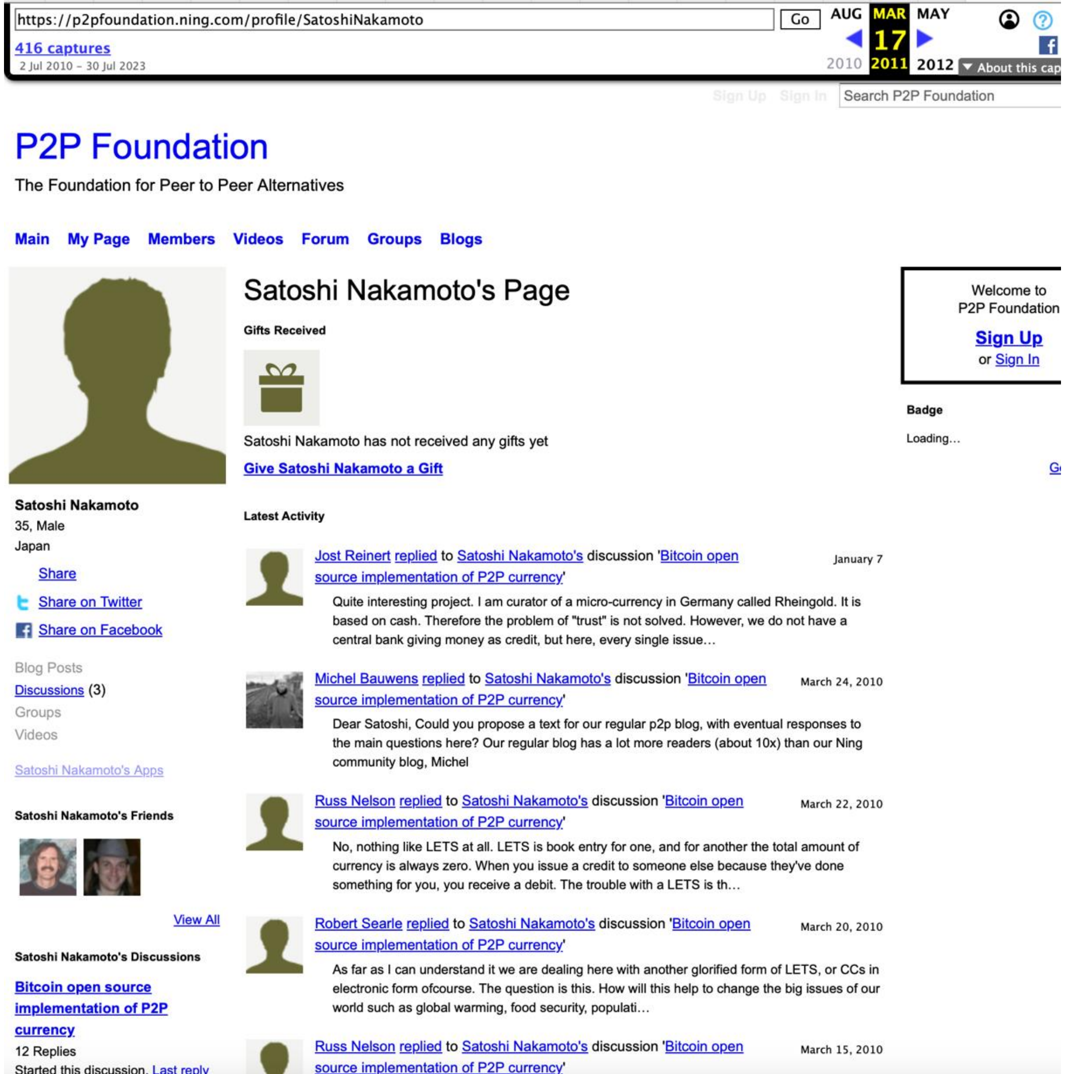
The most successful Blockchain Project

Bitcoin and Satoshi Nakamoto

Who’s Satoshi?

- Satoshi’s P2P Foundation profile: https://web.archive.org/web/20110317060514/https://p2pfoundation.ning.com/profile/SatoshiNakamoto
- Satoshi Nakamoto began coding the first implementation of Bitcoin in C++ in May of 2007.
- In August of 2008, he sent private emails to two well-respected cypherpunks, Hal Finney and Wei Dai, asking them for feedback on early versions of the Bitcoin white paper.
- They both gave Satoshi positive feedback, telling him they found it very promising.
- A couple months later, Satoshi published the Bitcoin white paper to a public cryptography mailing list.

Newsweek famously failed to uncover Satoshi Nakmoto’s identity in 2014: https://genius.com/Leah-mcgrath-goodman-the-face-behind-bitcoin-annotated



https://p2pfoundation.ning.com/profile/SatoshiNakamoto Go

416 captures
2 Jul 2010 – 30 Jul 2023

P2P Foundation

The Foundation for Peer to Peer Alternatives

Main My Page Members Videos Forum Groups Blogs

Satoshi Nakamoto's Page

Gifts Received

Satoshi Nakamoto has not received any gifts yet

Give Satoshi Nakamoto a Gift

Satoshi Nakamoto
35, Male
Japan

Share
Share on Twitter
Share on Facebook

Blog Posts
Discussions (3)
Groups
Videos

Satoshi Nakamoto's Apps

Satoshi Nakamoto's Friends

View All

Satoshi Nakamoto's Discussions

Bitcoin open source implementation of P2P currency
12 Replies
Started this discussion. Last reply

Latest Activity

Jost Reinert replied to Satoshi Nakamoto's discussion 'Bitcoin open source implementation of P2P currency' January 7

Quite interesting project. I am curator of a micro-currency in Germany called Rheingold. It is based on cash. Therefore the problem of "trust" is not solved. However, we do not have a central bank giving money as credit, but here, every single issue…

Michel Bauwens replied to Satoshi Nakamoto's discussion 'Bitcoin open source implementation of P2P currency' March 24, 2010

Dear Satoshi, Could you propose a text for our regular p2p blog, with eventual responses to the main questions here? Our regular blog has a lot more readers (about 10x) than our Ning community blog, Michel

Russ Nelson replied to Satoshi Nakamoto's discussion 'Bitcoin open source implementation of P2P currency' March 22, 2010

No, nothing like LETS at all. LETS is book entry for one, and for another the total amount of currency is always zero. When you issue a credit to someone else because they've done something for you, you receive a debit. The trouble with a LETS is th…

Robert Searle replied to Satoshi Nakamoto's discussion 'Bitcoin open source implementation of P2P currency' March 20, 2010

As far as I can understand it we are dealing here with another glorified form of LETS, or CCs in electronic form ofcourse. The question is this. How will this help to change the big issues of our world such as global warming, food security, populati…

Russ Nelson replied to Satoshi Nakamoto's discussion 'Bitcoin open source implementation of P2P currency' March 15, 2010

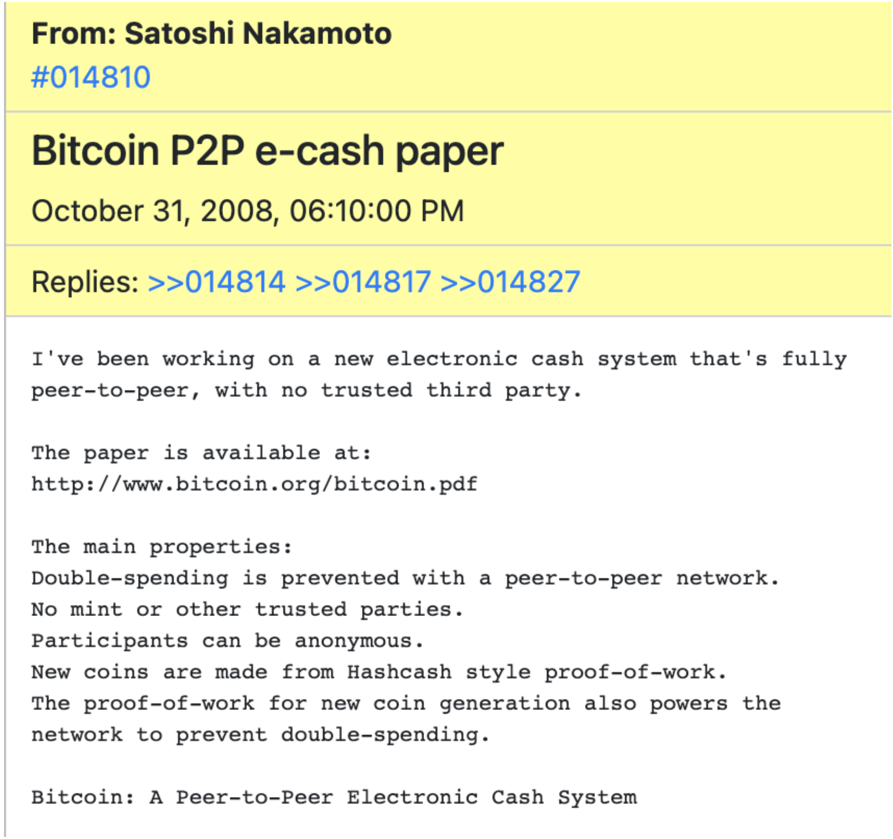
Welcome to
P2P Foundation

Sign Up
or Sign In

Badge

Loading…

Bitcoin: A Peer-to-Peer Electronic Cash System



From: Satoshi Nakamoto
#014810

Bitcoin P2P e-cash paper

October 31, 2008, 06:10:00 PM

Replies: >>014814 >>014817 >>014827

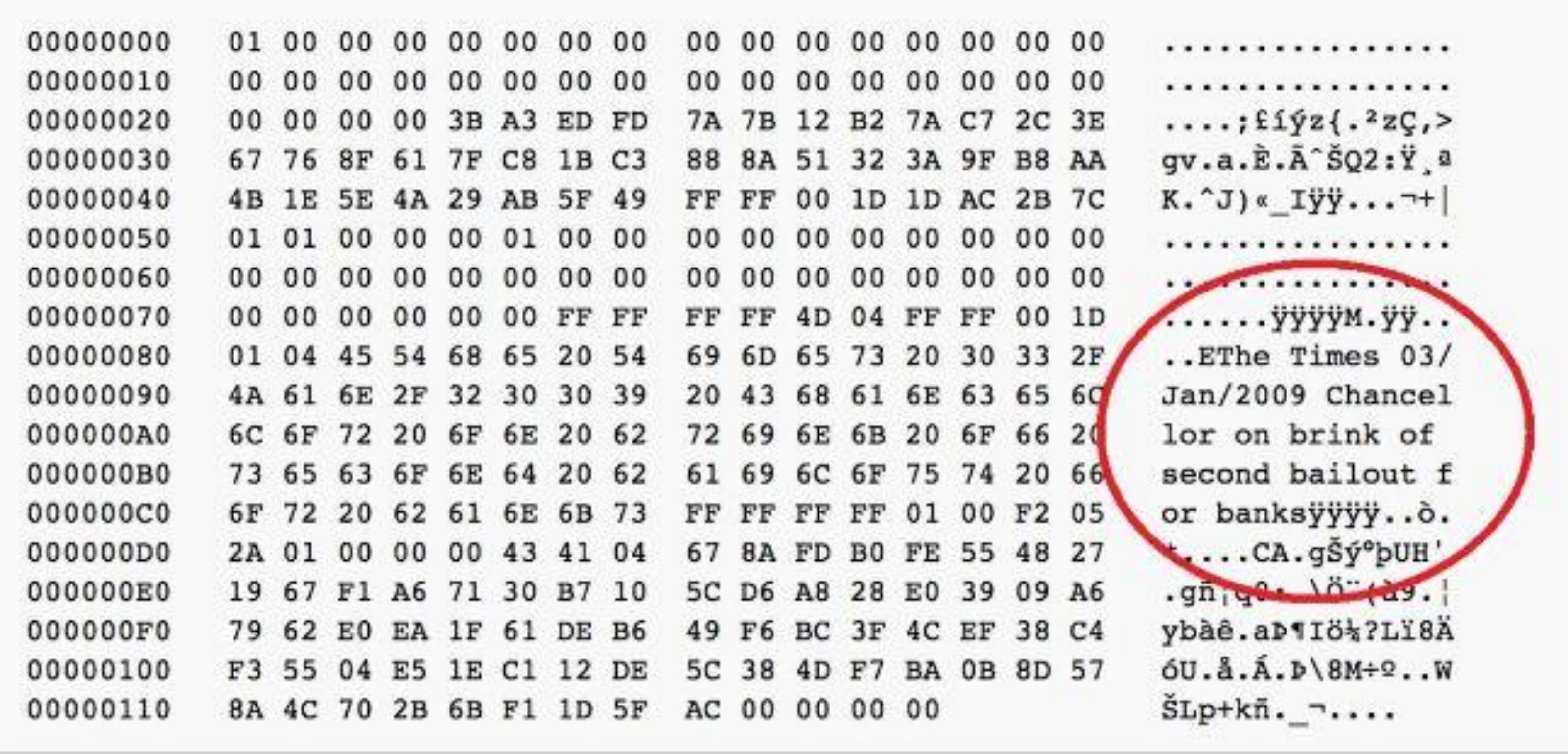
```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the
network to prevent double-spending.

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

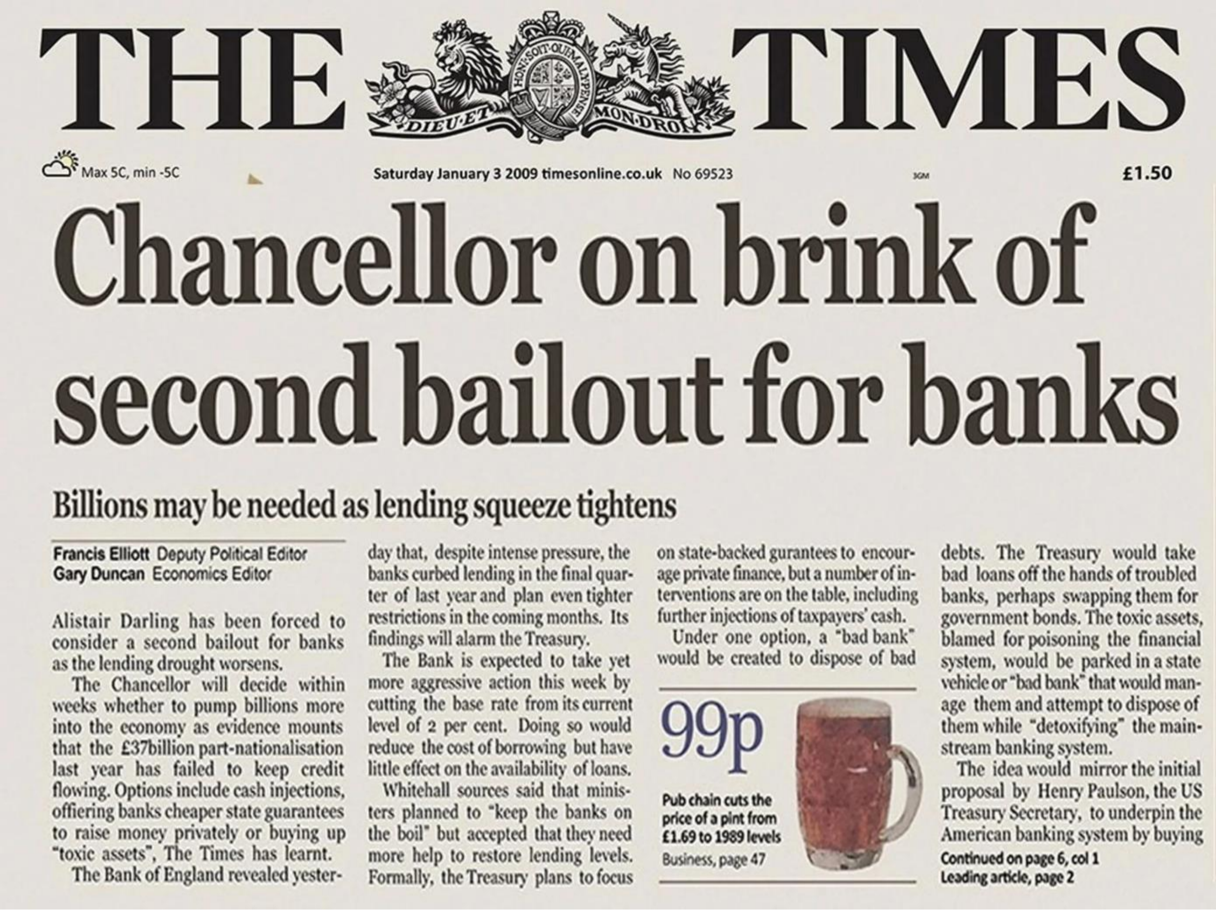
2026 Marks 17 Years of Bitcoin!



```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.ÃˆŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Bitcoin Genesis Block – Jan 03, 2009

RPI



THE TIMES

Max 5C, min -5C   Saturday January 3 2009 timesonline.co.uk No 69523   3GM   £1.50

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offiering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

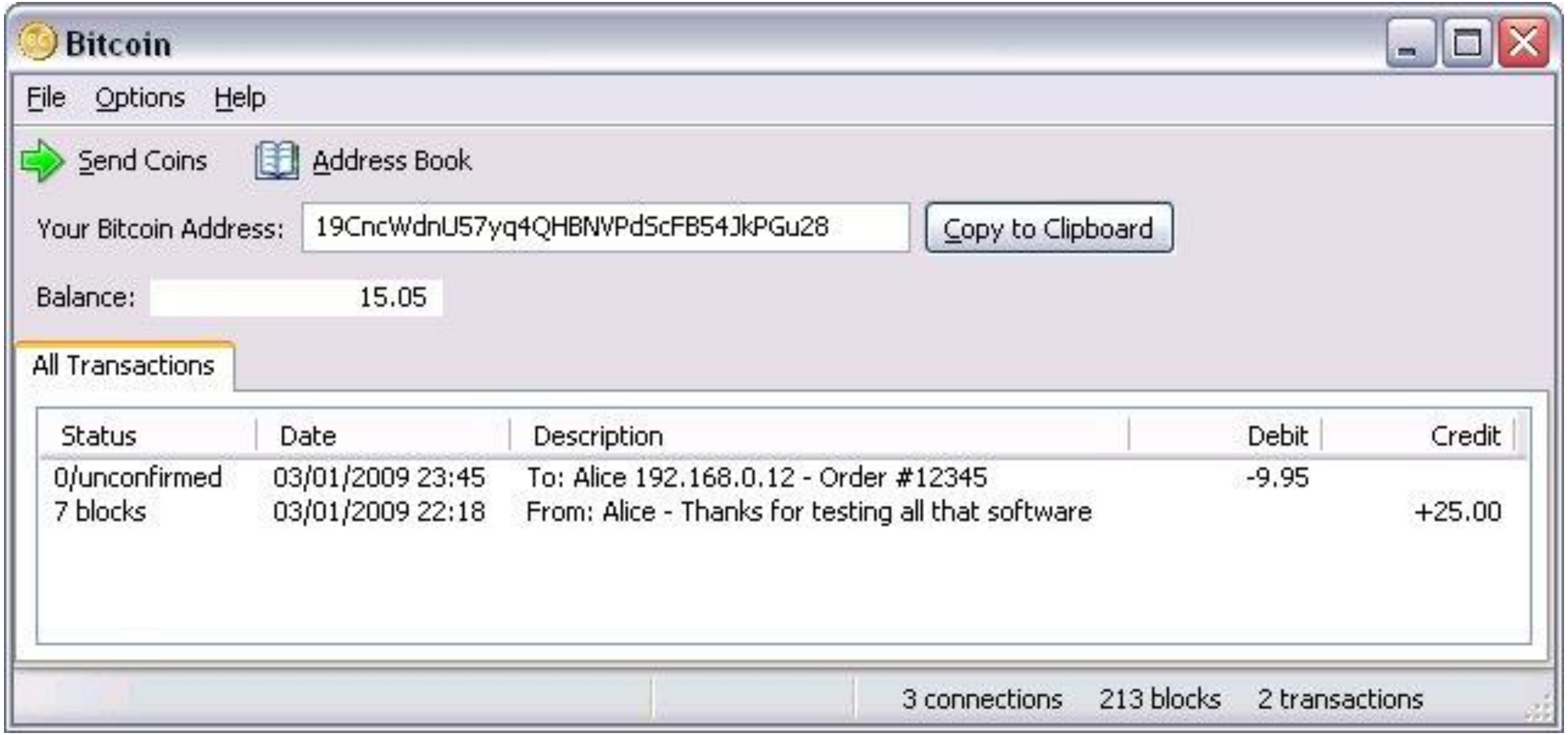
Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Early Bitcoin Days



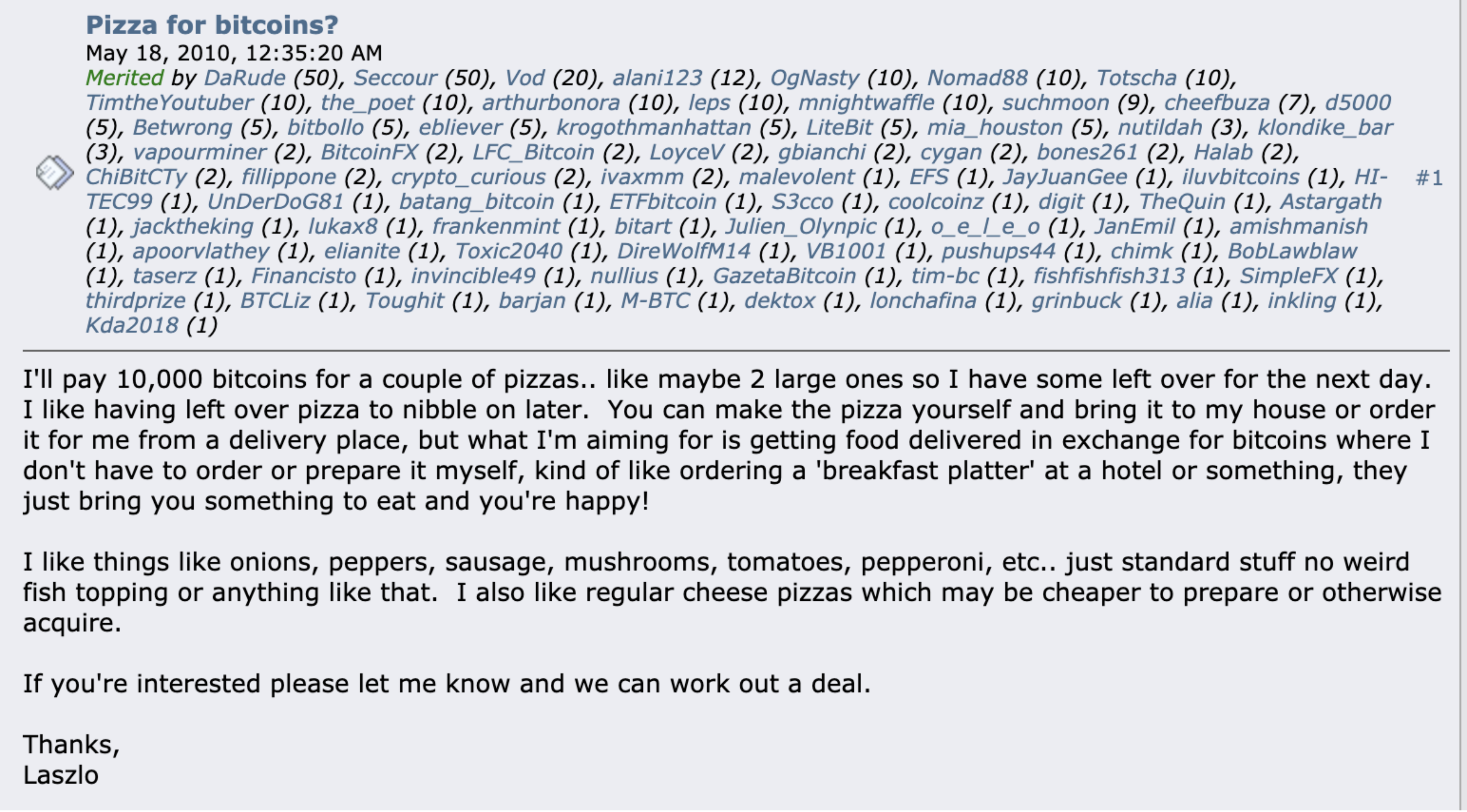
Your Bitcoin Address: 19CncWdnU57yq4QHBNVPdScFB54JkPGu28

Balance: 15.05

Status	Date	Description	Debit	Credit
0/unconfirmed	03/01/2009 23:45	To: Alice 192.168.0.12 - Order #12345	-9.95	
7 blocks	03/01/2009 22:18	From: Alice - Thanks for testing all that software		+25.00

3 connections 213 blocks 2 transactions

Snapshot of an early Bitcoin client. Credit: Deepceleron



Pizza for bitcoins?

May 18, 2010, 12:35:20 AM

Merited by *DaRude (50), Seccour (50), Vod (20), alani123 (12), OgNasty (10), Nomad88 (10), Totscha (10), TimtheYoutuber (10), the_poet (10), arthurbonora (10), leps (10), mnightwaffle (10), suchmoon (9), cheefbuza (7), d5000 (5), Betwrong (5), bitbollo (5), ebliever (5), krogothmanhattan (5), LiteBit (5), mia_houston (5), nutildah (3), klondike_bar (3), vapourminer (2), BitcoinFX (2), LFC_Bitcoin (2), LoyceV (2), gbianchi (2), cygan (2), bones261 (2), Halab (2), ChiBitCTy (2), fillippone (2), crypto_curious (2), ivaxmm (2), malevolent (1), EFS (1), JayJuanGee (1), iluvbitcoins (1), HI-TEC99 (1), UnDerDoG81 (1), batang_bitcoin (1), ETFbitcoin (1), S3cco (1), coolcoinz (1), digit (1), TheQuin (1), Astargath (1), jacktheking (1), lukax8 (1), frankenmint (1), bitart (1), Julien_Olynpic (1), o_e_l_e_o (1), JanEmil (1), amishmanish (1), apoorvlathey (1), elianite (1), Toxic2040 (1), DireWolfM14 (1), VB1001 (1), pushups44 (1), chimk (1), BobLawblaw (1), taserz (1), Financisto (1), invincible49 (1), nullius (1), GazetaBitcoin (1), tim-bc (1), fishfishfish313 (1), SimpleFX (1), thirdprize (1), BTCLiz (1), Toughit (1), barjan (1), M-BTC (1), dektox (1), lonchafina (1), grinbuck (1), alia (1), inkling (1), Kda2018 (1)*

#1

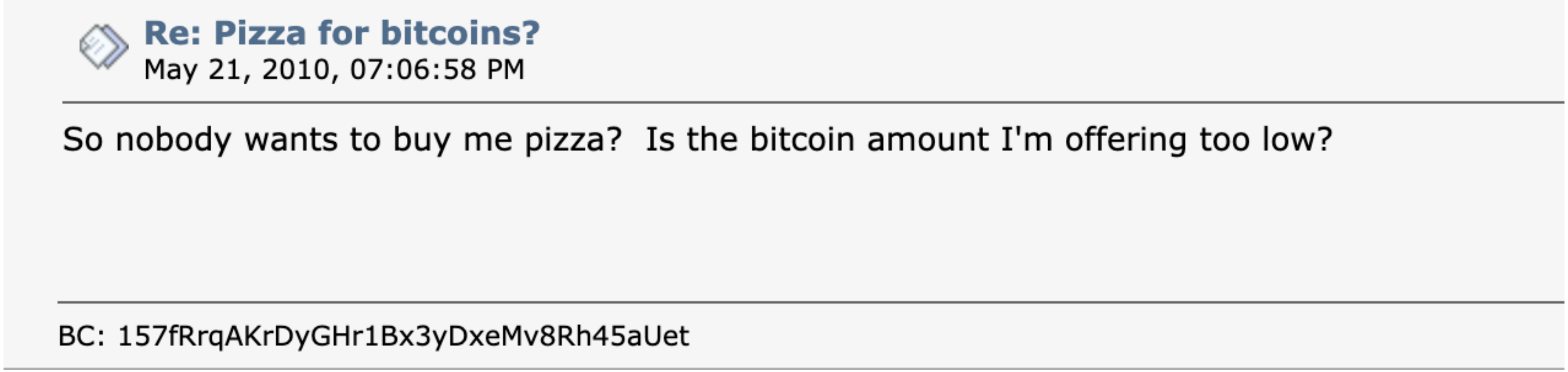
I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

https://bitcointalk.org/index.php?topic=137.0

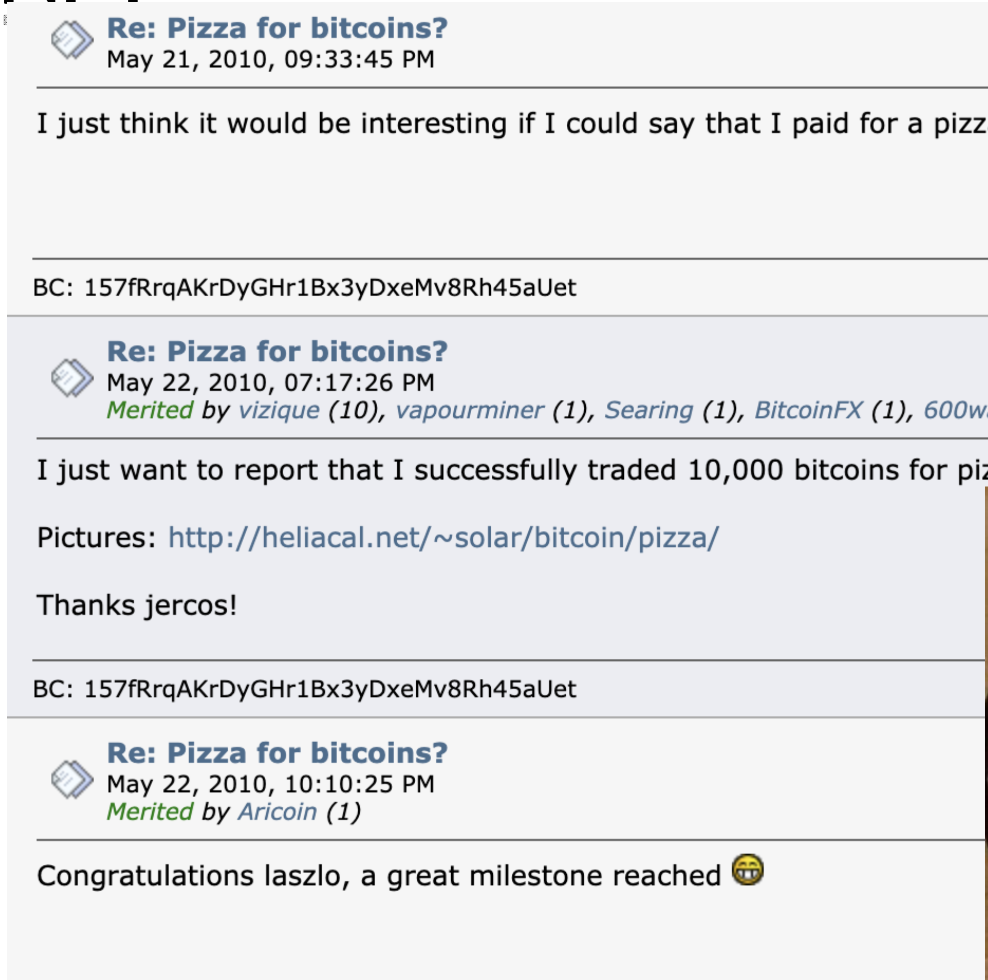


Re: Pizza for bitcoins?
May 21, 2010, 07:06:58 PM

So nobody wants to buy me pizza? Is the bitcoin amount I'm offering too low?

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

RPI



Re: Pizza for bitcoins?
May 21, 2010, 09:33:45 PM

I just think it would be interesting if I could say that I paid for a pizza in bitcoins 🙂

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM
Merited by vizique (10), vapourminer (1), Searing (1), BitcoinFX (1), 600watt (1), ETFbitcoin (1),

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

Re: Pizza for bitcoins?
May 22, 2010, 10:10:25 PM
Merited by Aricoin (1)

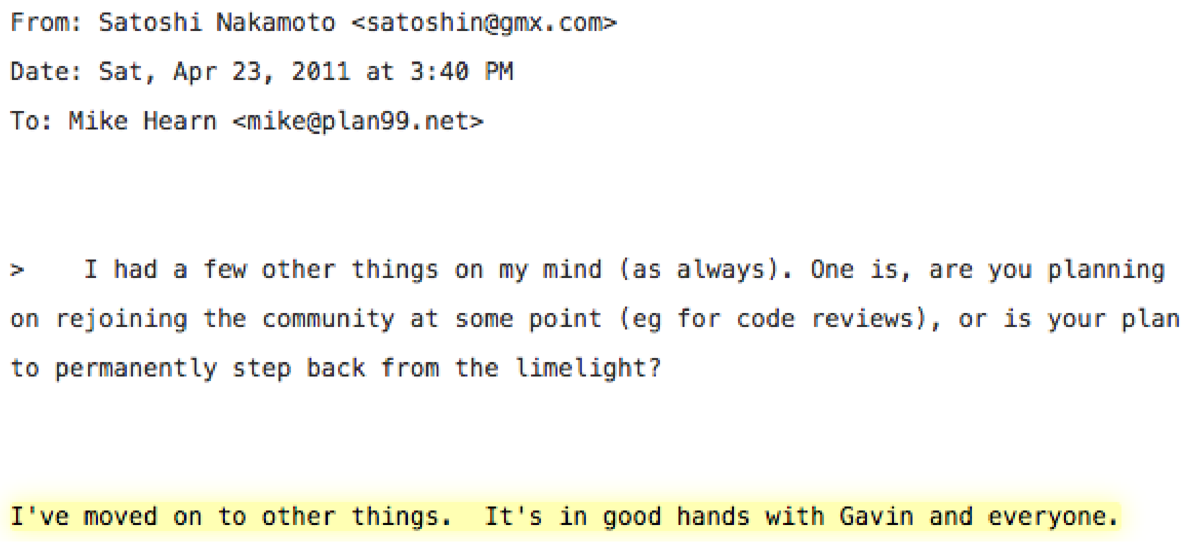
Congratulations laszlo, a great milestone reached 😁

Medium of Exchange

10,000 Bitcoins for 2 Pizzas

- **May 22, 2010: $41** ($20.50 per pizza)
- Mar 25, 2021: $522 million ($261 million per pizza)
- Sep 01, 2022: $200 million ($100 million per pizza)
- Jan 08, 2023: $169 million ($85 million per pizza)
- Sep 01, 2023: $260 million ($130 million per pizza)
- Jan 12, 2024: $434 million ($217 million per pizza)
- Jan 10, 2025, $948 million ($474 million per pizza)
- **Jan 13, 2026, $934 million ($467 million per pizza)**

No more Satoshi Nakamoto?



From: Satoshi Nakamoto <satoshin@gmx.com>
Date: Sat, Apr 23, 2011 at 3:40 PM
To: Mike Hearn <mike@plan99.net>

> I had a few other things on my mind (as always). One is, are you planning on rejoining the community at some point (eg for code reviews), or is your plan to permanently step back from the limelight?

I've moved on to other things. It's in good hands with Gavin and everyone.

One of Satoshi's last known emails

Satoshi’s Bitcoins: https://blog.bitmex.com/satoshis-1-million-bitcoin

Satoshi's addresses own about 600,000-700,000 BTC.

Discussion: why do you think Satoshi left the bitcoin project?

- No one knows for sure why Satoshi left the project.
- He grew bored?
- He saw Bitcoin's traction as a sign that the authorities would soon target him?
- He saw himself as more of a creator than a leader?
- He thought a project like Bitcoin would not succeed if it maintained a single leader, and the project's governance needed to be decentralized.

We'll likely never know for sure why Satoshi left!

Bitcoin’s Inspirations

Satoshi did not create Bitcoin from scratch but remixed many ideas that had never been combined before.

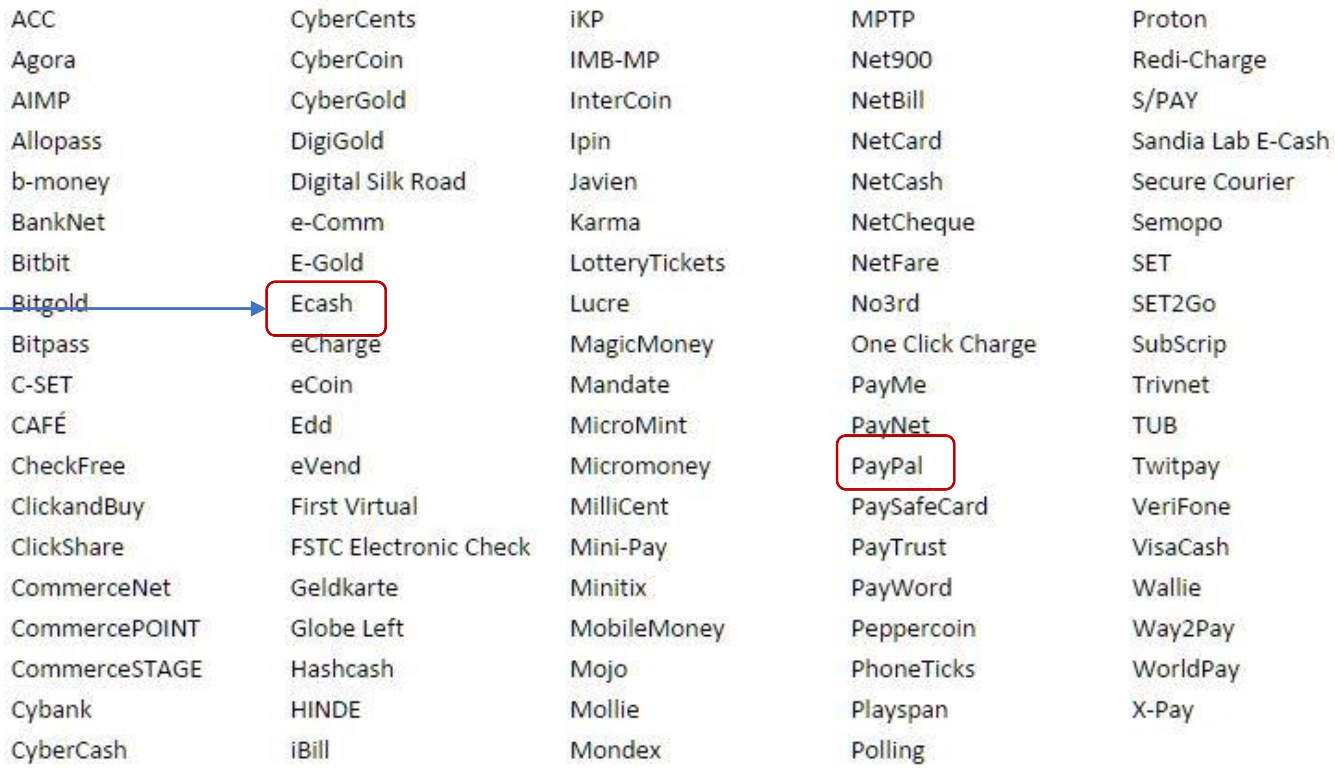
- **Ralph Merkle's work on Merkle trees**
  - Merkle, Ralph C. "A digital signature based on a conventional encryption function." *Conference on the theory and application of cryptographic techniques*. Springer, Berlin, Heidelberg, 1988.
- **Haber and Stornetta's work on cryptographic timestamping services**
  - Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." *Conference on the Theory and Application of Cryptography*. Springer, Berlin, Heidelberg, 1990.
- **Hashcash by Adam Back**
  - ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf
- **b-money by Wei Dai**
  - http://www.weidai.com/bmoney.txt

Bitcoin’s Primary Innovation:

- Proof of Work Consensus (now called ***Nakamoto Consensus***)

The Long Road of Cryptocurrencies

Digicash
Chaum et al
1986



ACC
Agora
AIMP
Allopass
b-money
BankNet
Bitbit
Bitgold
Bitpass
C-SET
CAFÉ
CheckFree
ClickandBuy
ClickShare
CommerceNet
CommercePOINT
CommerceSTAGE
Cybank
CyberCash

CyberCents
CyberCoin
CyberGold
DigiGold
Digital Silk Road
e-Comm
E-Gold
Ecash
eCharge
eCoin
Edd
eVend
First Virtual
FSTC Electronic Check
Geldkarte
Globe Left
Hashcash
HINDE
iBill

iKP
IMB-MP
InterCoin
Ipin
Javien
Karma
LotteryTickets
Lucre
MagicMoney
Mandate
MicroMint
Micromoney
MilliCent
Mini-Pay
Minitix
MobileMoney
Mojo
Mollie
Mondex

MPTP
Net900
NetBill
NetCard
NetCash
NetCheque
NetFare
No3rd
One Click Charge
PayMe
PayNet
PayPal
PaySafeCard
PayTrust
PayWord
Peppercoin
PhoneTicks
Playspan
Polling

Proton
Redi-Charge
S/PAY
Sandia Lab E-Cash
Secure Courier
Semopo
SET
SET2Go
SubScrip
Trivnet
TUB
Twitpay
VeriFone
VisaCash
Wallie
Way2Pay
WorldPay
X-Pay

Which ones do you recognize?

Paper to Read For Next Class

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

https://bitcoin.org/bitcoin.pdf

Oshani will lead the discussion, and the next class’s quiz will be based on these contents.

For all the remaining classes, we will assign the presenters to lead the paper discussion.

Group Activity: Design the Blockchain for X

In groups of two discuss a design for a blockchain for some use case X.

X can something like (or any other impactful application):

- Decentralized identity for refugees
- DeFi lending protocol for volatile markets
- Blockchain for scientific publishing / peer review
- Supply chain transparency for critical minerals
- DAO governance for public infrastructure
- AI model provenance & auditing

Group Activity: Design the Blockchain for X

- **Why blockchain?**
  - What problem *cannot* be easily solved with a centralized system?
- **Core design choices**
  - Consensus mechanism (and why)
  - On-chain vs off-chain components
  - Privacy level (transparent vs private vs selective disclosure)
- **Key trade-offs** Identify **at least two tensions**, e.g.:
  - Scalability vs decentralization
  - Transparency vs privacy
  - Governance efficiency vs inclusiveness
- **Failure mode / attack vector**
  - What is the *most likely* way this system fails or is exploited?
- **Open research question**
  - What is one *unsolved problem* that would make a good research paper?

Today’s “Quiz”

https://bit.ly/4aTDkww