

Frontiers in Blockchain Research

How to read a paper &

Bitcoin: A Peer-to-Peer Electronic Cash System

Class 02
Jan 16, 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:** LOW 4034
- **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 (Updated)

4000 Level

- Paper Presentations: 30%
- Class Participation: 20%
- Project: 50%
- Paper: optional (strongly encouraged)

6000 Level

- Paper Presentations: 20%
- Class Participation: 20%
- Project: 40%
- 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.



Tentative Topics

Week	Theme
1–2	Origins & Foundations (Bitcoin, Time-Stamp, Consensus)
3–4	Consensus Mechanisms Deep Dive
5	Smart Contracts & Ethereum
6	Cryptography & Privacy
7	Scalability & Layer-2
8	Economics, Governance & Regulation
9	Applications (Finance, Healthcare, Supply Chains)
10 - 14	Emerging Research

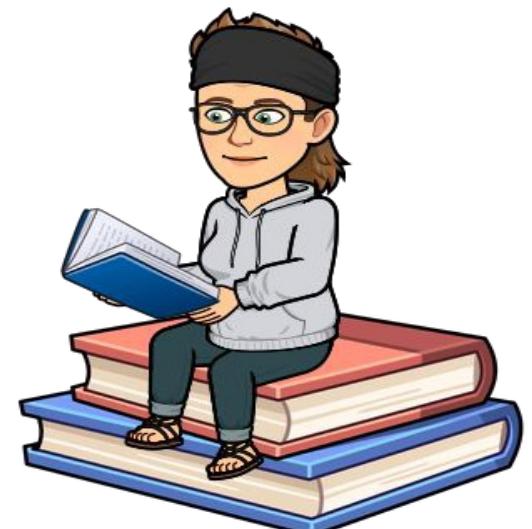
How to read a research paper

The following slides are adapted from:

https://serc.si.edu/sites/default/files/website-gen/how_to_read_a_scientific_paper_ksm_v.1.pptx.pdf

Challenges to reading a scientific paper

- Not taught how to read them
- Not an expert in the field
- Technical language
- Hard to understand graphics and statistics
- Sounds like a different language/not accessible



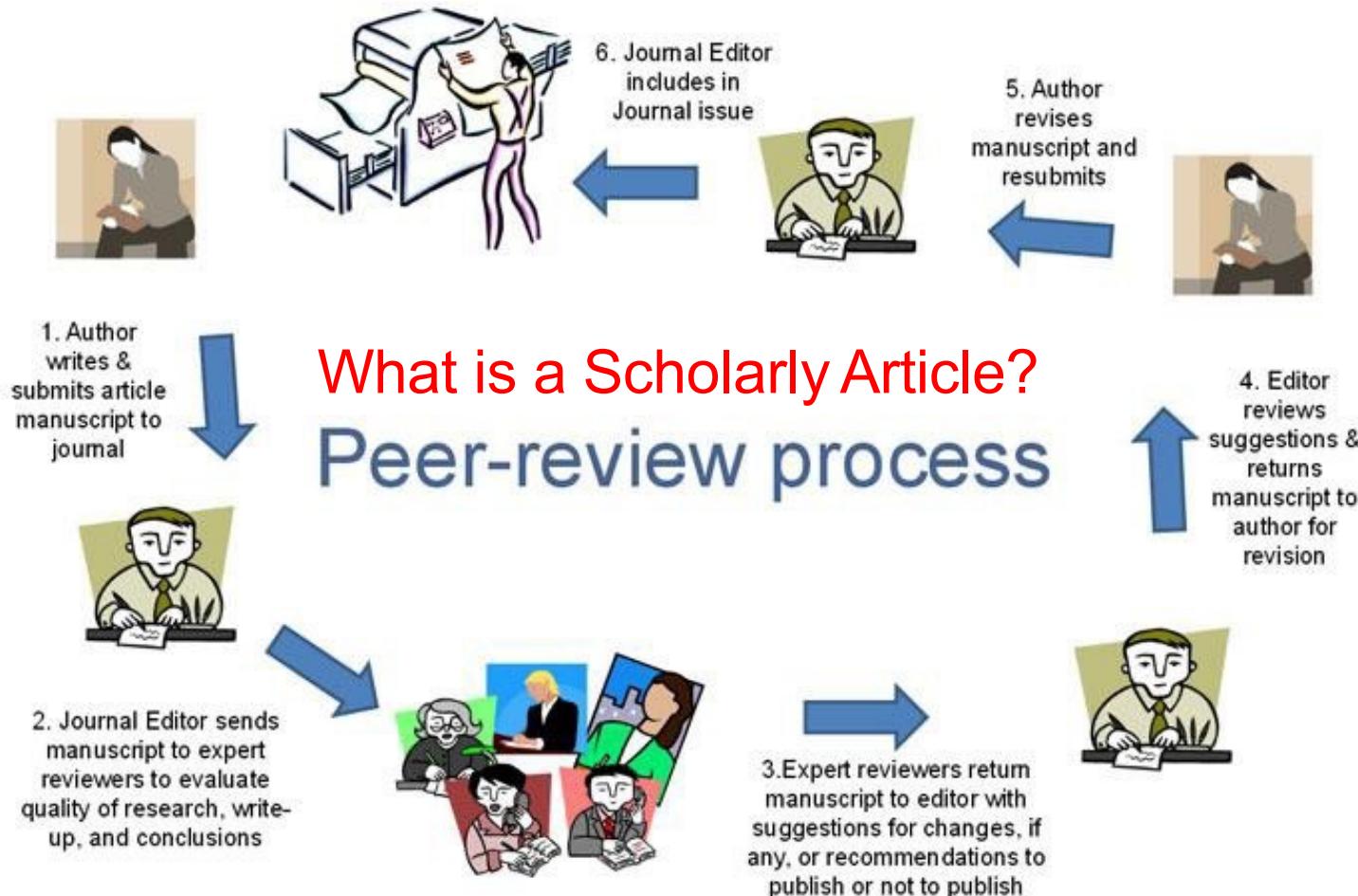
What are the categories of written scientific information resources? (*frequently updated*)

- Newspapers and magazines
- Blogs and online articles
- Journals
- Peer-reviewed or scholarly journals



When you do online searches:

- A. Limit searches to peer-reviewed journals only (use a filter)
<https://www.jstor.org/>
- B. Articles written by academics and/or professionals (though “expert” isn’t always an accurate title)



What is a Scholarly Article? Peer-review process

HINT: Not all information in a peer-reviewed journal is peer-reviewed!

Sometimes editorials, letters to the editor, book reviews, and such are in the journal, but they aren't counted as peer-reviewed articles.

Why Read a Scientific Paper?

Is there a good reason to
read the literature?

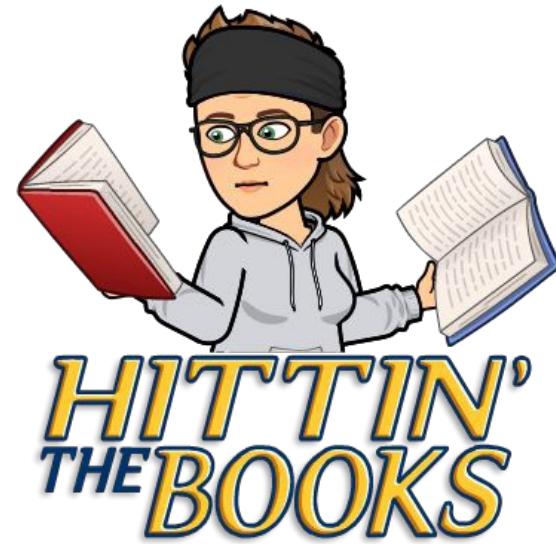


Why Read?

It's Current!

Textbooks can be years out of date by the time they are published. Journals tell you what is happening...

RIGHT NOW!



Why Read?

It's Current!

It Can Be Replicated!



Popular articles and books give you general information and results. Scholarly journals give you enough information that

you could do the experiment yourself.

You can verify the research to see if you get the same results.

Why Read?

It Has Actual Data!



If you need to know **exact results or properties** for your own research...

Articles include actual data, uncertainties, conditions of the experiment, and much more.

Why Read?

It's Current!
You Can Evaluate The Conclusions!

Do You Believe It... Or Not?

Articles provide the authors' explanation of their results and conclusions. You can see their assumptions and determine whether you believe them or not.



RPI

Let's put a
pin in That



Why Read?

So, There You Have It...

Current

It's the most up to date stuff

Has Raw Data

Save time - use their results

Replicable

I can redo the experiment
myself

Shows Logic

Do you believe it... or not?

All the Reasons to Read Scientific Papers

How To Read...

Before you read, you need the right equipment....

A Scientific Dictionary:

- Look up terms you don't know.
- Try <https://www.thesciencedictionary.com> for an online dictionary.
- Or simply search (or ask a genAI tool – but do watch out for hallucinations.
- Reading online is helpful, because you can copy and paste as you go.

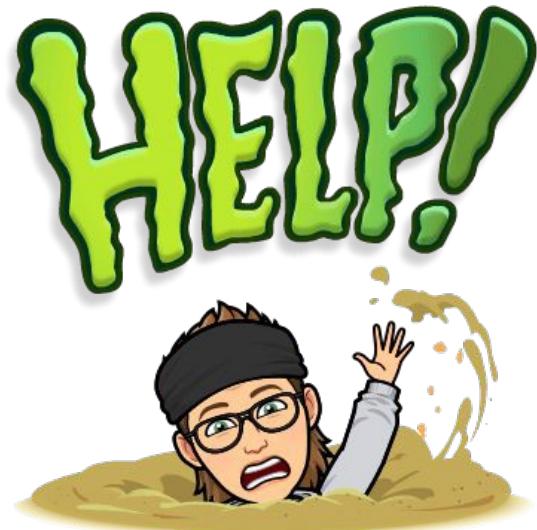
Your handy-dandy notebook:

- Make notes so you'll remember your insights. Add a highlighter, pen or marker.

Your friends and colleagues:

- Explaining to others will help you understand the paper yourself.

Don't Read Straight Through!



It's like drowning in quicksand!

Give yourself a task while reading,

- *taking notes

- *looking up terms you don't know

- *writing information and questions in the margins.

- Save informative sentences in your notebook.

- Be patient with yourself

- Print and highlight

Have a clear idea about the information that you need or want



For blockchain research

You might want to:

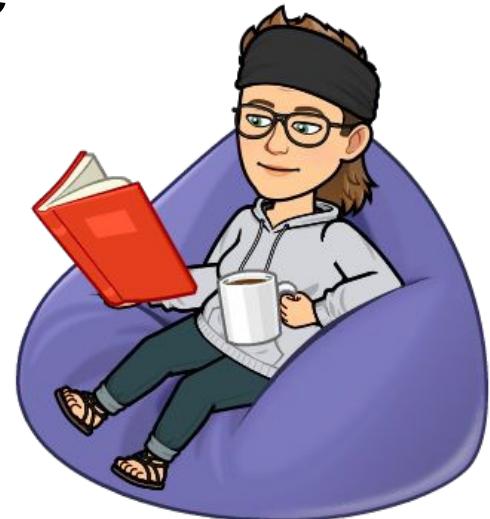
- Start with the problem the paper is trying to solve, not the specifics of the protocol.
 - Is this a **new problem**, or a **new solution to a known problem?**
- Blockchain papers live or die by their assumptions.
 - Identify the threat model and assumptions
- **Red flag:** claims without formal definitions or proofs.
- Understand the evaluation: what is actually being measured?

For blockchain research

- Look for trade-offs (there is no free lunch): ask “does this paper improve X at the cost of Y?”
 - Scalability vs decentralization
 - Privacy vs auditability
 - Security vs latency
 - Governance flexibility vs stability
- Distinguish theory from practice.
 - Is this protocol deployable today?
 - What hidden costs exist (communication, storage, governance)?
 - Does the paper assume “honest behavior” where incentives suggest otherwise?

The Title, Authors, Publisher and Year

- Make sure the authors are credible
- Is there one author or many?
- What year was the paper written?
- Where was the paper published?
- Is it a credible source? Publisher?



The Abstract

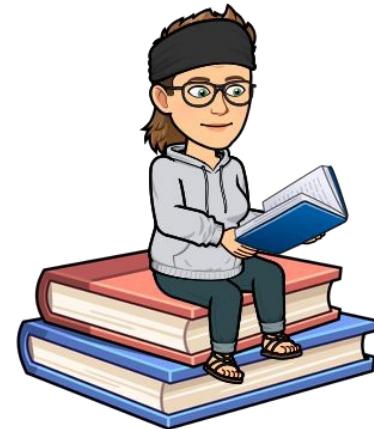
Gives you a **brief overview** of what the paper is all about (hypothesis, methodology, and results)

Explains **why** the authors did the experiment, **how** they did it, and **what they found out and what it means**.

It's very important to read abstracts to help you decide **whether to read** the whole paper or not.

Abstracts are **available in many indexes** to the journal literature, so you don't even need to find the actual article to determine whether it might be interesting to read.

HINT: Abstracts may be bold, italicized, or unlabeled.



The Introduction

Provides the motivation for doing the experiment, explaining '**Why did they bother?**'

Gives you background and context

It gives you background, **explains prior research**, and what the accepted understanding of the field is.



Will often end with the hypothesis of the study.

RPI

Methods (super dense)

Skip this section until last.

Gives details on how the experiment was set up and carried out. Methods, techniques, scope

Should explain well enough that **you could replicate** the experiment yourself, if you wanted to.

Often the hardest section to understand, since it contains specialized techniques.

When reading, skim and **try to pick out basic methods** used. Don't worry that much about the details.

Consult a scientific encyclopedia or textbook if you don't understand the concepts of the technique.



Results

This section provides the **data the authors use** to reach their conclusions.

Figures are often included to **make the data more compact** and intuitive, and **Tables organize data** in one place for easier reading.

Understanding Figures and Tables is **EXTREMELY** important in understanding a paper.

For figures, make sure you understand what quantities are on the axes. Are they linear or logarithmic? What units are plotted?



Discussion/Analysis/Conclusion

(This section may be named any of these things)

This is where the author connects the dots - explaining what the data means, and why they support the conclusion. Also provide context and how results measure up to the hypothesis.

Compare your own conclusions about the data with the authors' analysis.

When skimming the paper for the first time, after reading the abstract **read the concluding section.** It gives more detail on the specific results that were found, and **helps you determine whether the paper is relevant** to your research question.



RPI

References/Bibliography

Provides a list of resources quoted or referenced by the authors.

Allows you to go back to those sources to **see why the authors referenced** that work, and **whether those sources seem reliable** and accurate.

Format of bibliography differs between journals. **Author. (Year) Journal Title. Volume(Issue): pages.**



Read the abstract

- Look for main points, look up terms, see what they concluded

Read the conclusion/Discussion

- What did the scientists conclude?
- Did it make sense?
- Do you need to read another section or graphs to understand?

Look at plots and figures

- Know what the axes mean, and what scale they are
- Facts/data don't lie, but the abstract and conclusion can be bent to fit

Lastly look at the introduction and methods

Strategies for Reading

Some people start by Reading very fast, and then Rereading.



RPI Strategies for Reading

As you read, ask yourself, “Do I need to understand this part to continue on?”

- Reflect on what you read
- Draw your own conclusions
- Do you believe the credibility of the research?
- How do these results relate to my interests?
- Read the paper again

READ



<https://www.sciencemag.org/careers/2016/01/how-read-scientific-paper>

Where to Find Articles

- Libraries
- Online at researcher's website
- Journals online
- Free libraries online or in person
- Google Scholar





What are your strategies for reading papers?



Activity: let's explore a blockchain

<https://andersbrownworth.com/blockchain>

Bitcoin: A Peer-to-Peer Electronic Cash System

RPI

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 Nakamoto's identity in 2014:
[https://genius.com/Leah-mcgrath-goodman-the-face-behind-bitcoin-³⁴
annotated](https://genius.com/Leah-mcgrath-goodman-the-face-behind-bitcoin-annotated)

<https://p2pfoundation.ning.com/profile/SatoshiNakamoto> [Go](#) **AUG** **MAR** **MAY**
17 **2011** **2012** [About this page](#)

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](#)

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...

[View All](#)

Satoshi Nakamoto's Discussions

[Bitcoin open source implementation of P2P currency](#)

12 Replies
Started this discussion. [Last reply](#)

 [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 of course. 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

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

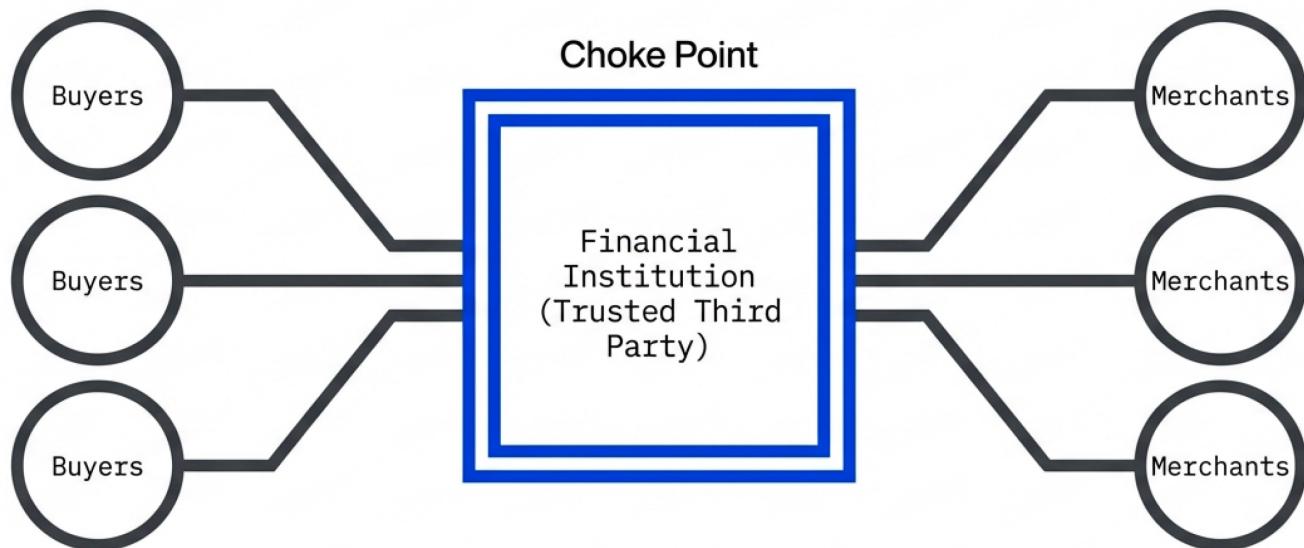
I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

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

The Inherent Weakness of the Trust-Based Model



Non-Reversible Transactions

Impossible. Financial institutions cannot avoid mediating disputes.

Transaction Costs

Mediation increases costs, limiting minimum transaction size.

Privacy Loss

Merchants must validate customer identity to guard against fraud.

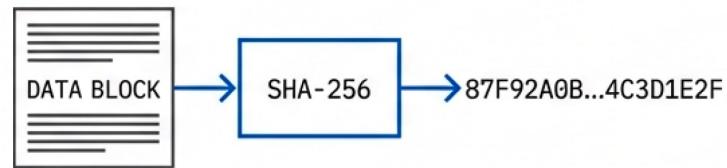
Replacing Trust with Cryptographic Proof

The Trust Model (Status Quo)



Relying on a central authority
to verify every transaction

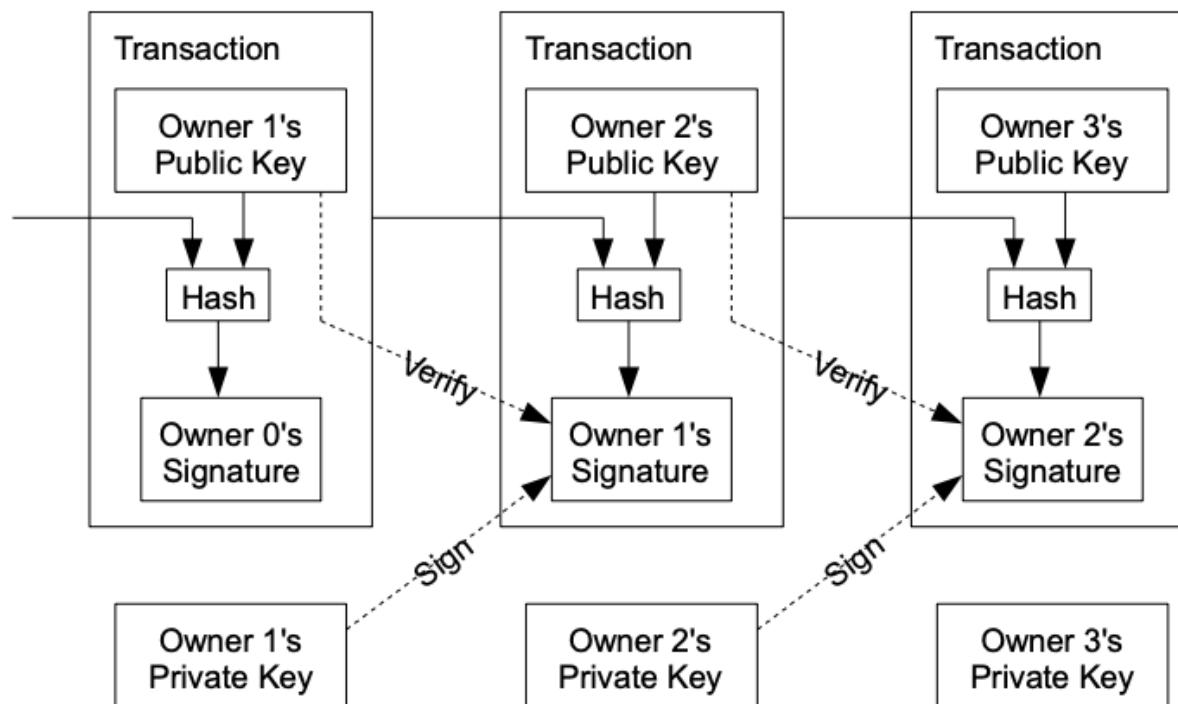
The Proof Model (Bitcoin)



Relying on a peer-to-peer distributed
timestamp server to generate
computational proof of chronological order

The system is secure as long as honest nodes collectively control more
CPU power than any cooperating group of attacker nodes.

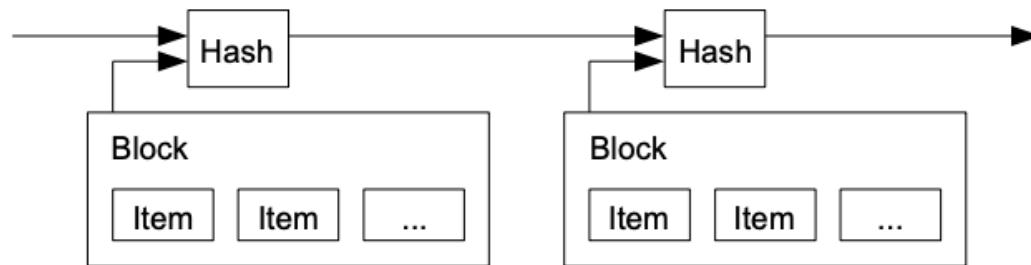
Electronic coin as a chain of digital signatures



The challenge

- Digital signatures verify ownership, but they do not prove a coin hasn't been spent already.
- Common solution:
 - A central Mint checks every transaction (centralized)
- Bitcoin solution:
 - Transactions must be publicly announced.
 - Participants agree on a single history of the order in which they were received.

Establishing Time: The Timestamp Server



- A timestamp server takes a hash of a block of items and publishes it.
- Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

Proof-of-Work (PoW)

PoW is computational proof that some work has been performed.

Usually, this is implemented through a computational puzzle.

The puzzle should be:

- easy to state (*find me a needle in this haystack*)
- hard to solve (*the haystack is big*)
- easy to verify (*yep, that's a needle*)

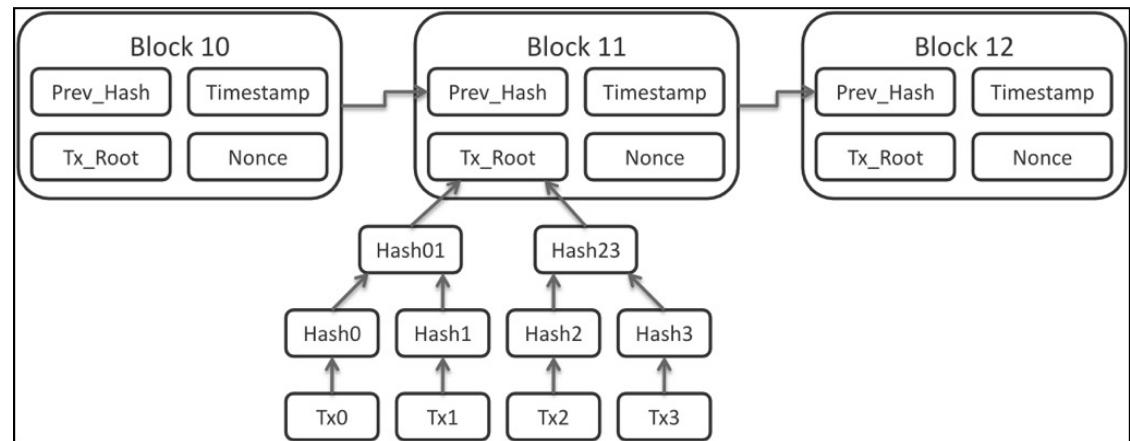


Generating a solution to the puzzle serves as evidence that the solver performed some work.

Proof of Work (PoW)

- A given node collects transactions that are broadcast to the entire network and stores them in a block
 - Before including transactions in the block, the node verifies that the transactions are valid
 - Invalid transactions result in a block being rejected by the other nodes

- The transactions are typically assembled in a type of Merkle tree



Proof of Work (PoW)

- The transactions pay a fee to the mining node to be included the transaction, higher fees are included first
- The mining node begins solving an extremely difficult cryptographic hashing problem, with the transactions being part of the input to the problem
 - This is essentially a guessing game with a very low chance of guessing correctly
 - Once the correct answer is known, it is very easy for other people to check that it works
 - Part of the motivation for solving the problem is the rewards the miner receive

Example “Computational Puzzle”

- The computer must find a hash value meeting the following target criteria (known as the difficulty level):

SHA256("blockchain" + Nonce) = Hash Digest starting with **“000000”**

- The text string “blockchain” is appended with a nonce value, and then the hash digest is calculated.
- The nonce values used will be numeric values only.

SHA256("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938 (not solved)

SHA256("blockchain1") =
0xdb0b9c1cb5e9c680dff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10 (not solved)

...

SHA256("blockchain10730895") =
0x**000000**ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587 (solved)

- Each additional “leading zero” value increases the difficulty.

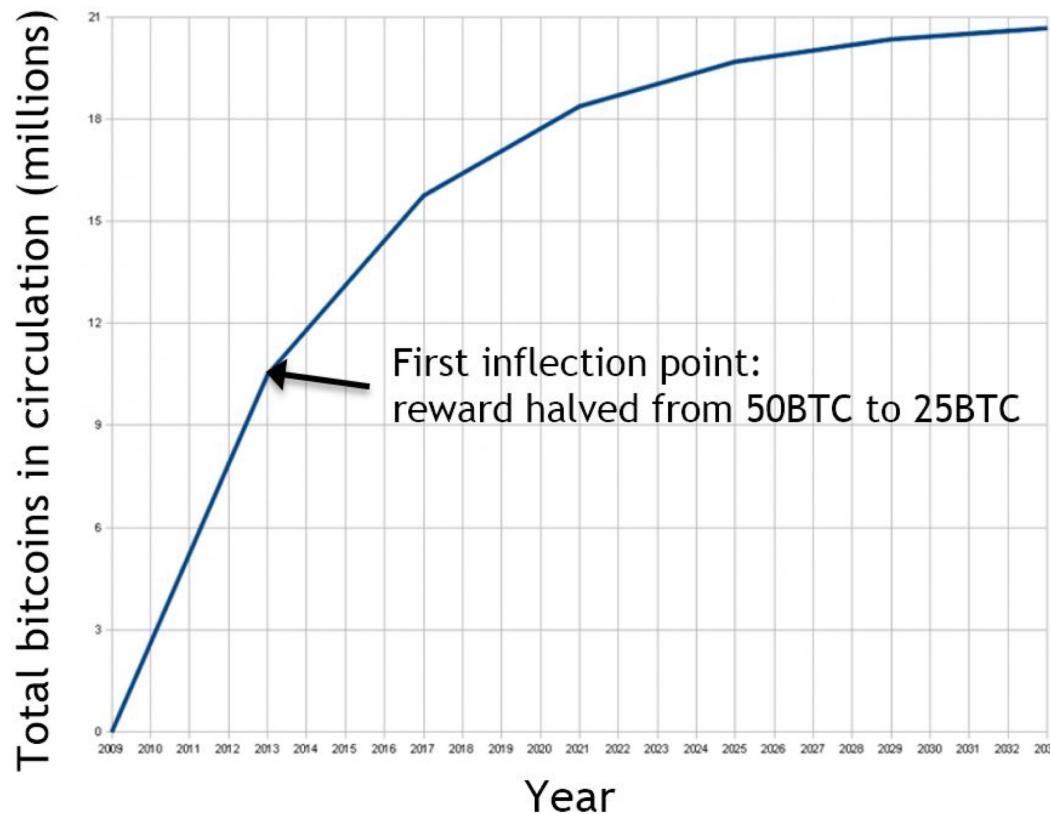
Proof of Work (PoW)

- The mining node that has found the correct solution broadcasts it to the rest of the network, and begins the next block with another complex cryptographic hashing problem
- The longest blockchain (weighted by work) is always taken to be the correct chain, and thus the other miners will also begin the new problem: the length of each block is determined by how much work it took to create
- The other nodes can quickly check that the transactions included in the block are valid, and that the broadcast solution is actually a solution to the problem.
 - Verification of the nonce is easy since only a single hash needs to be done to check to see if it solves the puzzle.

Bitcoin Halving

- A Bitcoin halving event is when the reward for mining Bitcoin transactions is cut in half.
- When Bitcoin first started, 50 Bitcoins per block were given as a reward to miners.
- After every 210,000 blocks are mined (approximately every 4 years), the block reward halves and will keep on halving until the block reward per block becomes 0 (approximately by year 2140).
- This event also cuts in half Bitcoin's inflation rate and the rate at which new Bitcoins enter circulation.
- Previous halvings have correlated with intense boom and bust cycles that have ended with higher prices than prior to the event.
- Bitcoin last halved on 05 May 2024 12:27:18 UTC, resulting in a block reward of 3.125 BTC.

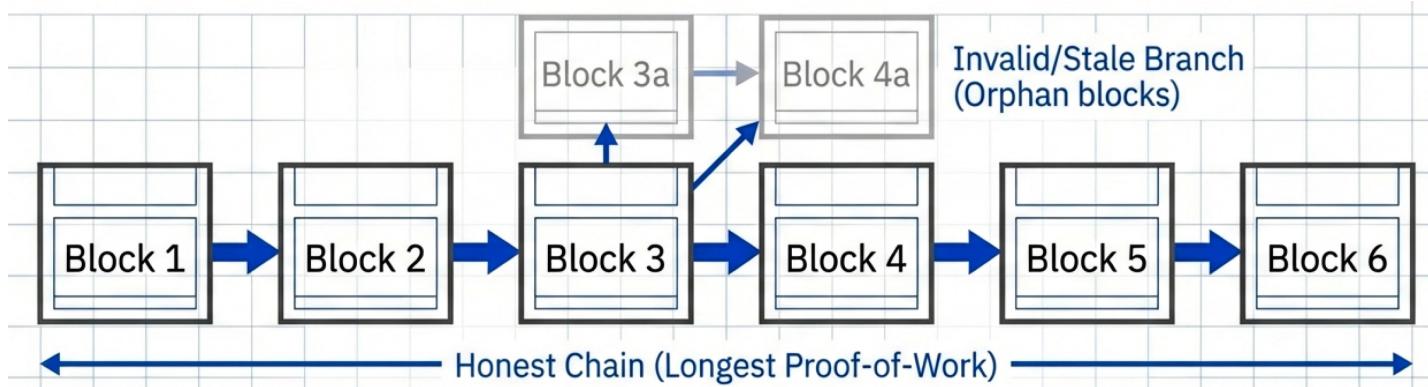
PoW Incentives with Bitcoin as an Example



Mining Pools

- Nodes organize themselves into “pools” or “collectives,” whereby they work together to solve puzzles and split the reward.
- Work can be distributed between two or more nodes across a collective to share the workload and rewards
- For example:
 - Node 1: check nonce 0000000000 to 0536870911
 - Node 2: check nonce 0536870912 to 1073741823
 - Node 3: check nonce 1073741824 to 1610612735
 - Node 4: check nonce 1610612736 to 2147483647
- What about “Sybil Attacks”?
 - PoW combats this by having the focus of **network influence** being the **amount of computational power** (hardware, which costs money) mixed with a **lottery system** (the most hardware increases likelihood but does not guarantee it)

The Longest Chain Rule: One CPU One Vote

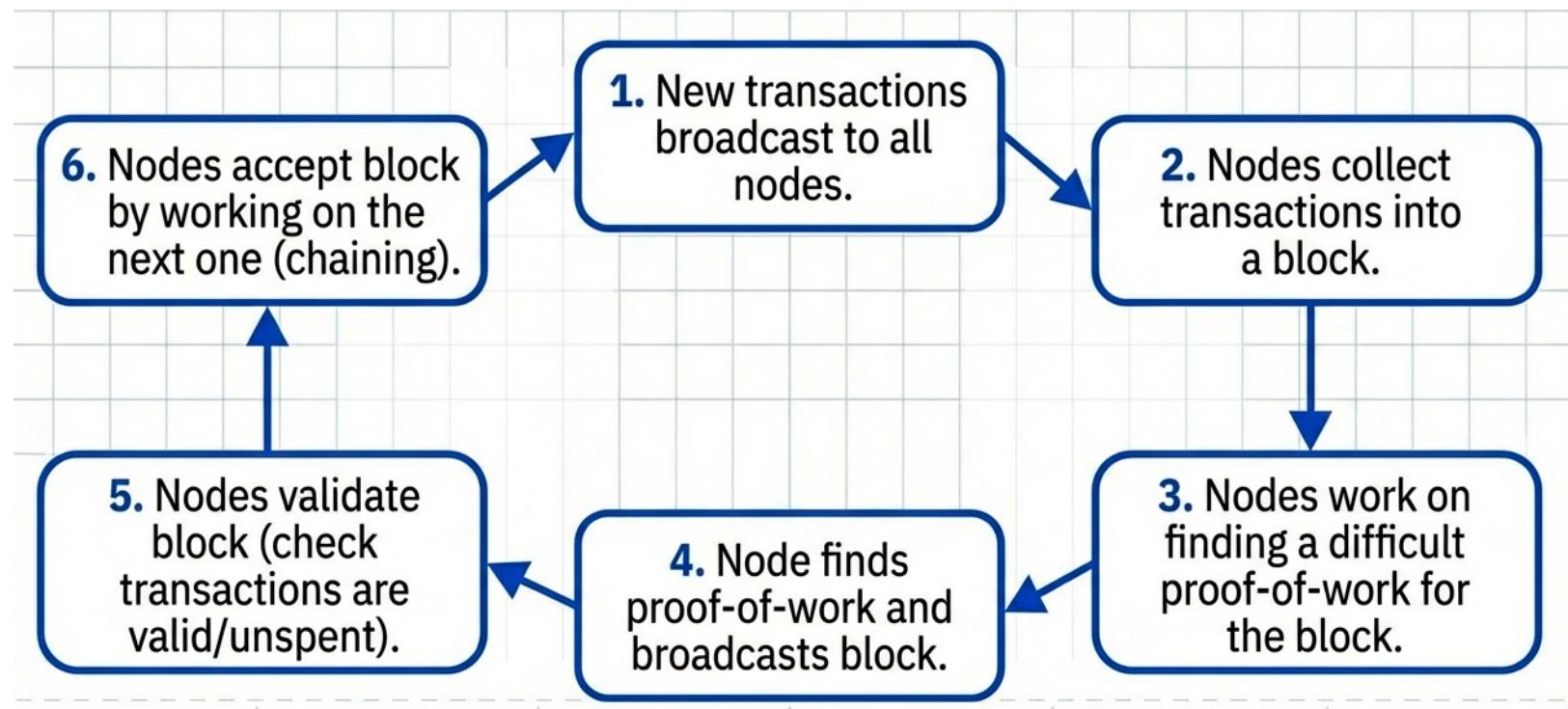


The voting problem: if the majority were based on one IP address one vote, it could be subverted by anyone allocating many IPs. (Sybil Attack)

The solution: PoW is essentially one CPU one vote.

Consensus: The majority decision is represented by the longest chain, which has the greatest PoW invested in it.

Network Operations



PoW Strengths

- Proven reliability
- Predictable block times
- Robust, and does not rely on any other node being trustworthy
- Cannot be censored
 - Public transactions can be seen as a drawback in some cases

PoW Drawbacks



- The need for specialized hardware, i.e., Application Specific Integrated Circuit (ASIC)
- Energy Costs
- The only known vulnerability is the so-called '**51% attack**'
 - One miner or group of miners is able to take over the resources driving the chain forward.
 - However, expenditure of large computing and energy cost to take 51% would be lost if crypto collapsed. Historical example, **alchemists**.
- Mining pools are able to slightly game the system by **delaying the release of a found block** and gaining a slight head start on the next one
- Scalability issues
 - Lower transaction throughput
 - Lowering the block time (problem difficulty) is potentially less secure
- Miners often sell the coins immediately, removing any loyalty to the chain they are mining

2026 Marks 17 Years of Bitcoin!

00000000	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 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	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	7A 7B 12 B2 7A C7 2C 3E;fíýz{..²zç,>
00000030	67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA	88 8A 51 32 3A 9F B8 AA	gv.a.È.À~SQ2:Ý,a
00000040	4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iýý...~+
00000050	01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 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	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	FF FF 4D 04 FF FF 00 1DýýýýM.ýý..
00000080	01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F	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	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	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	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	FF FF FF FF 01 00 F2 05	or banksýýýý..ò.
000000D0	2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27	67 8A FD B0 FE 55 48 27CA.gSýºþUH'
000000E0	19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6	5C D6 A8 28 E0 39 09 A6	.gn,ç, ö, »~(19.1
000000F0	79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4	49 F6 BC 3F 4C EF 38 C4	ybàë.aþIÖ?LÝ8Ä
00000100	F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57	5C 38 4D F7 BA 0B 8D 57	óU.å.Á.þ\8M+?..W
00000110	8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00	AC 00 00 00 00	SLp+kñ. ~....

Bitcoin Genesis Block – Jan 03, 2009

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, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt. The Bank of England revealed yester-

day 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 guarantees 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

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

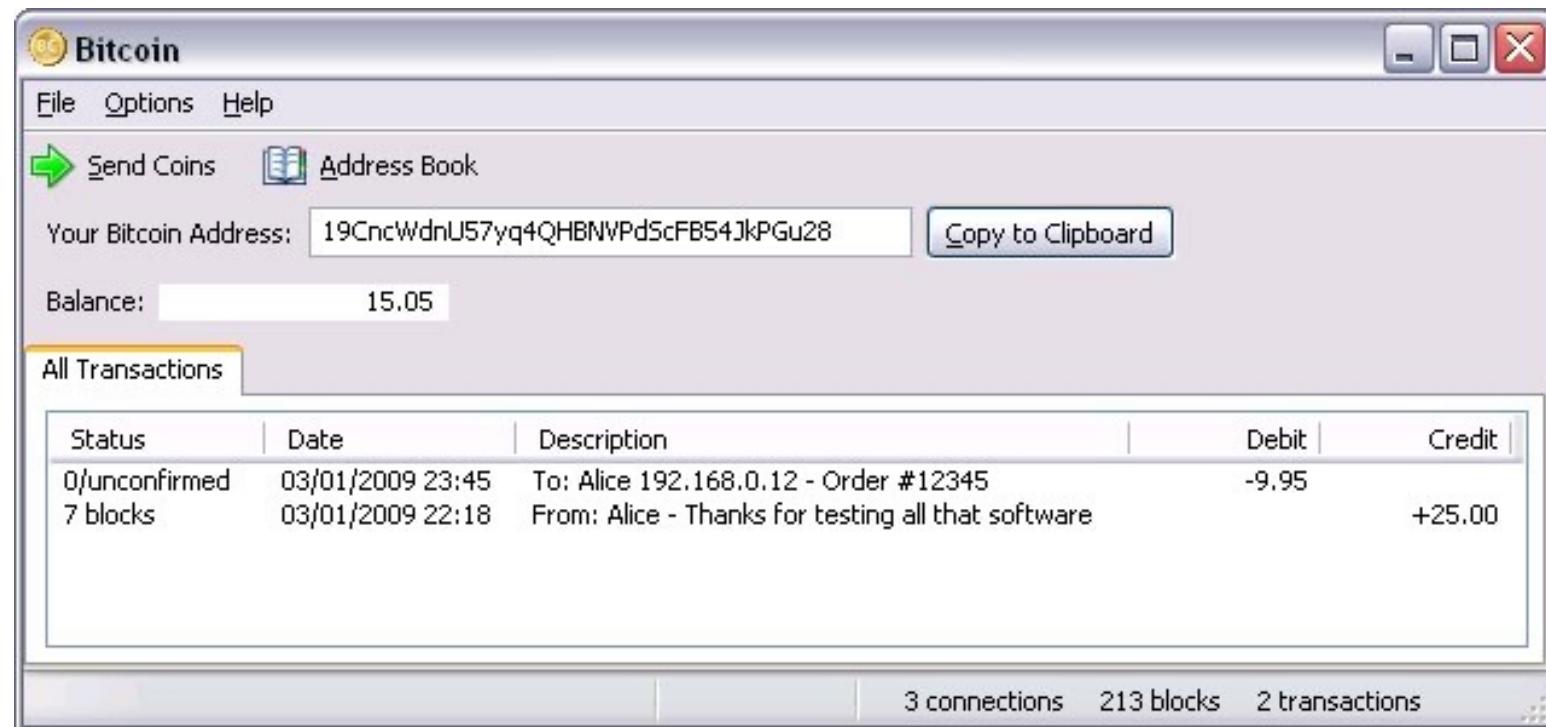
debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying"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



Early Bitcoin Days



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), [arthurbanora](#) (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), [HITEC99](#) (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), [apoovrlathey](#) (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), [dektok](#) (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), *ETFBTC* (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 😊





Next Tuesday's Paper

Stuart Haber & W. Scott Stornetta, “How to Time-Stamp a Digital Document” (1991) — early description of linking cryptographically hashed timestamps

<https://link.springer.com/article/10.1007/BF00196791>