

The Yale University logo, a large blue 'Y' with a white outline, is centered in the background of the slide.

CPSC 3640/5400: Decentralized Payments, Contracts, and Finance for Humans and AI

Welcome and Course Introduction

Fan Zhang
Yale University
2026 Fall

Logistics

- You know the location and time
- CPSC 3640 v.s. 5400
 - Different workloads (e.g., additional HW questions)
- Briefly about myself
 - more at <https://fanzhang.me>
- Course website
 - Schedule
 - Lecture notes
 - Reading materials
- Canvas (assignments)
- Gradescope (submissions)

CPSC 3640 / CPSC 5400

Decentralized Payments, Contracts, and Finance for Humans and AI

Announcements

- CPSC 3640 / CPSC 5400 will be offered in Fall 2026. The course website is now live with the schedule and logistics.

Course Information

Time/location • MW, 11:35am-12:50pm • 17 Hillhouse Avenue 113	Platforms • Canvas
Instructor  Prof. Fan Zhang Office hours: TBD, TBD	Teaching Assistance  TBA

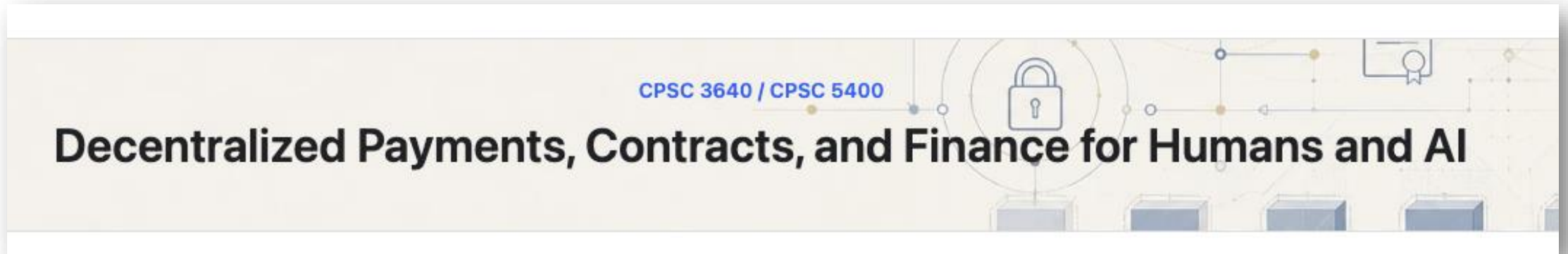
Course Description

Blockchains provide a platform for humans to coordinate economic activity without relying on centralized intermediaries. Emerging standards as EIP-8004 aim to extend these capabilities to autonomous agents, enabling AI systems to transact and coordinate through shared protocols. This introductory course explores such decentralized applications, including tokens, exchanges, lending protocols, stablecoins, oracles, decentralized governance, and emerging standards for AI coordination and interoperability. Students will learn system architecture, security intuition, and how to build and debug decentralized applications.

► [Course Units \(click for details\)](#)

Remember the URL:
<https://cpsc3640.netlify.app>

What is this course about?



- It's about
 - technologies behind decentralized implementation of financial services...
 - ...and their applications for humans ...
 - ...and AI agents

Finance

- What is Finance?
 - the process that involves the creation, management, and investment of money and financial assets
- Financial assets/financial instruments
 - a non-physical asset whose value is derived from a contractual claim
 - Examples: Bank deposits, stocks, bonds, loans, derivatives
- Financial services
 - banking, lending/borrowing, exchange, payments, etc
- Traditional financial services are provided by “centralized” institutions:
 - Banks, Exchanges, Payment companies, etc

Features & issues of Centralized Finance

- Hold custodies of customers' funds/assets. They are trusted to operate correctly
 - Well, they are not the most trustworthy people
- Serves as intermediaries for transactions
 - can censor/block transactions or charge high fees (rent seeking)
- Adhere to strict on-boarding & continuous compliance rules (regulation)
 - compliance enforcement can be slow and ineffective.
- Customer has no privacy to service provider: Service provider knows **real identity** and full **transaction history**
 - E.g., insider attacks, database leaks
- Siloed databases and applications
 - Lack of openness hinders innovation and collaboration



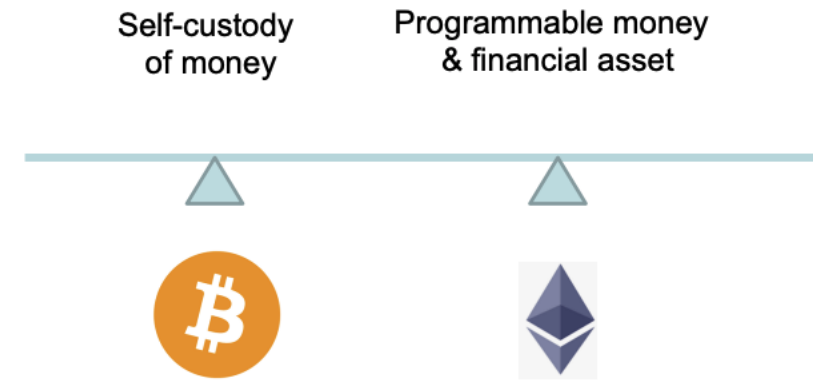
Decentralized Finance Advantages

We will learn DeFi's advantages over CeFi, including

- **non-custodial** finance services
- **ensorship resistance**
- fast and **cheap** transactions [e.g. the cost is the same be it a \$3 or \$3m transaction]
- automatic and provable **compliance**
- Financial **privacy** with support for **compliance**
- open **interoperability** between services
- no need for trust, because anyone can **verify**

Decentralized Finance (DeFi)

- DeFi: Payments, contracts, and other finance services implemented by on decentralized **smart contract** platforms.
- Bitcoin: Birth of (public) blockchains
- Ethereum: Birth of smart contract platform
- Key feature: Strong **integrity** and **availability**
 - E.g., even the developer can't alter or stop the programs once deployed.



DeFi adoption examples (digital assets)

- E.g., cryptocurrencies, stablecoins, NFTs
- Bitcoin and Ethereum ETFs (Exchange-Traded Funds)
 - bring crypto investing into mainstream finance.
- Stablecoins (eg USDC)

Statement on the Approval of Spot Bitcoin Exchange-Traded Products



**U.S. Securities and
Exchange Commission**

Will Schmitt in New York JULY 22 2024

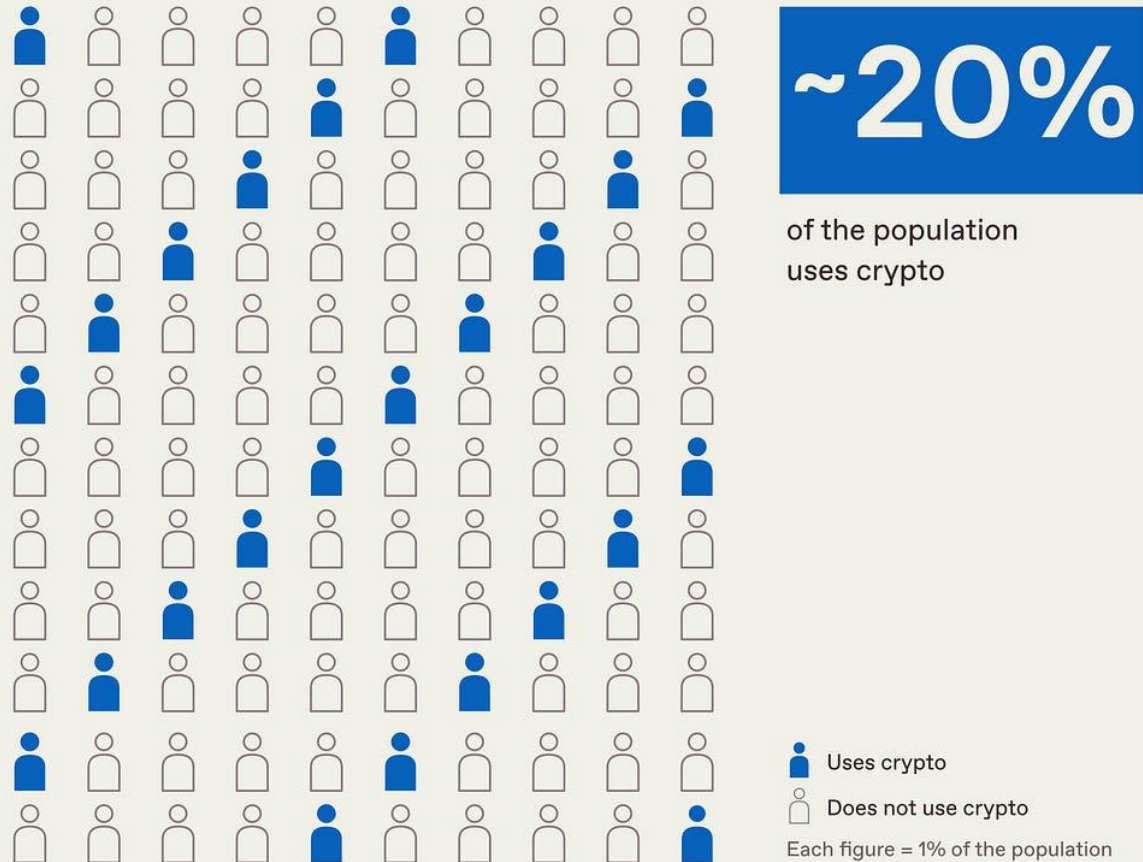
FINANCIAL TIMES

**SEC approves ether ETFs as crypto moves
closer to mainstream**

Latest authorisations follow January launches of first US spot bitcoin ETFs

One in five Argentines now uses crypto

Crypto users as share of population, 2025



- One in five Argentines uses crypto, with major crypto-app downloads rising 93% in 2024.
- Stablecoin salary payments increased alongside inflation, helping workers preserve purchasing power.
- Stablecoins receive 94% of Argentine peso crypto flows because “buying crypto” usually means buying digital dollars.
- Stablecoins provided 24/7 access to dollars when capital controls restricted the official foreign-exchange market.
- Usage persists as inflation falls, suggesting stablecoins are becoming everyday financial infrastructure

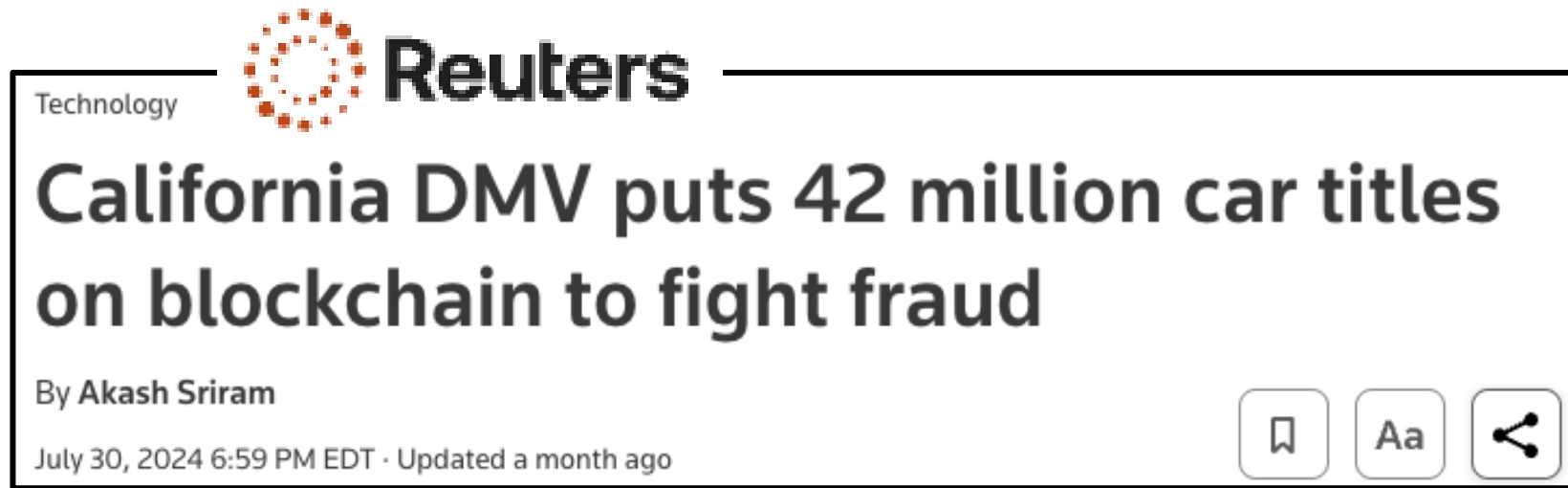
<https://a16zcrypto.substack.com/p/how-argentina-uses-crypto-in-5-charts>

Institutional adoption news (2026)

- Asset management: **BlackRock** manages nearly \$80 billion in digital-asset ETPs and operates the world's largest tokenized Treasury fund.
- Bank payments and treasury: **JPMorgan's Kinexys** processes more than \$7 billion per day in payments and tokenized-asset transactions.
- Bond issuance: **HSBC Orion** has facilitated more than \$5 billion of digital-bond issuance, including government bonds.
- Interbank infrastructure: **Swift** has completed its blockchain ledger and 17 banks are preparing initial transactions.
 - <https://www.blackrock.com/corporate/investor-relations/larry-fink-annual-chairmans-letter>
 - <https://www.jpmorgan.com/kinexys/index>
 - <https://www.business.hsbc.com/en-gb/insights/hsbc-approved-for-digital-securities-sandbox>
 - <https://www.swift.com/news-events/press-releases/swifts-blockchain-ledger-ready-use-17-banks-set-pioneer-tokenised-cross-border-payments-trusted-global-infrastructure>

Other (non-monetary) use cases

Distributed ledger can be used for identity/naming systems



WorldID

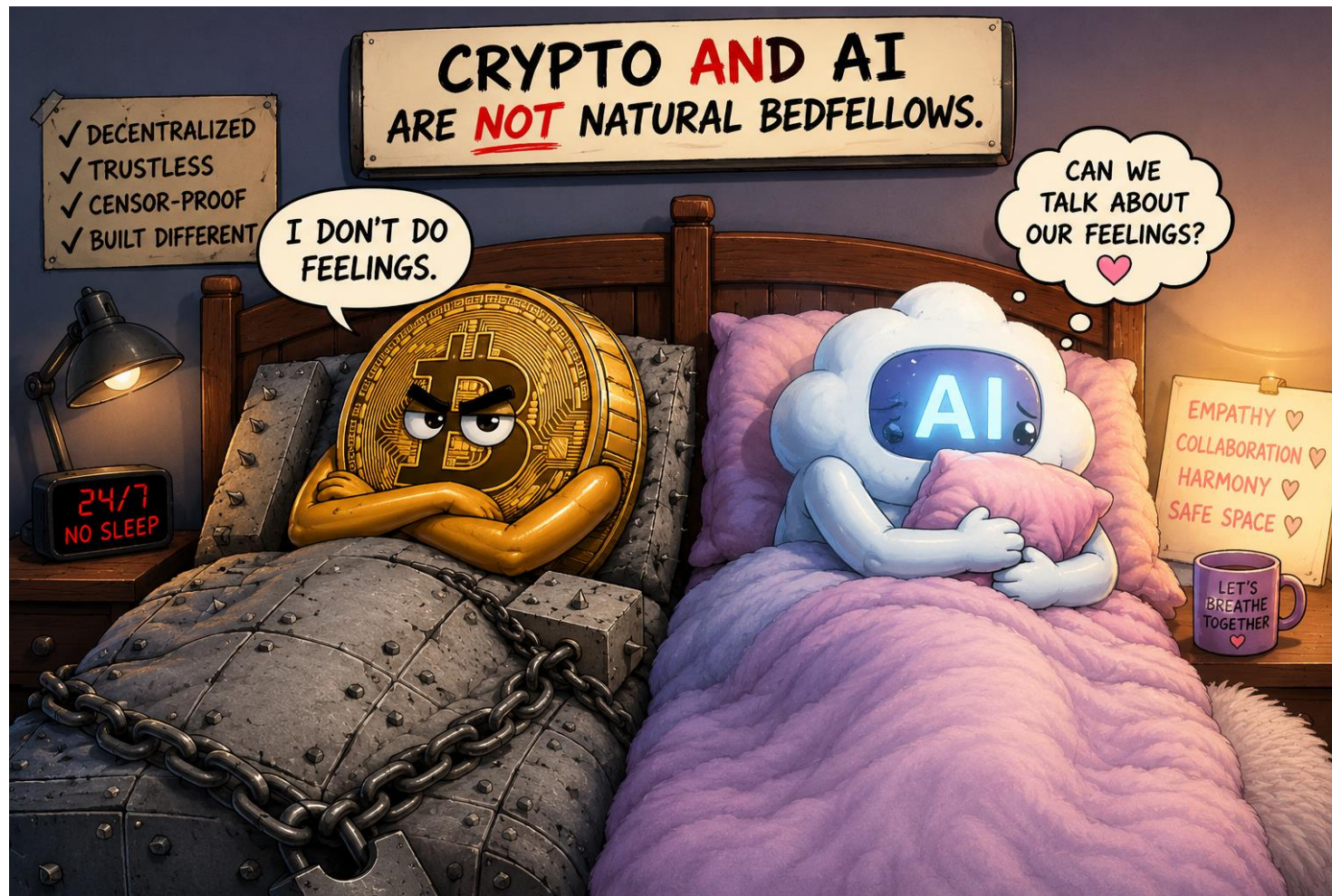


- Mission: “create a global ‘proof-of-human’ identity network (World ID) to distinguish real people from bots as AI becomes more ubiquitous.”
- Co-founder: Sam Altman!

DeFi also comes with a new set of risks

- Technological risks
 - Extremely unforgiving for **bugs** (because bugs $\Rightarrow$ \$\$\$)
 - Now AI can find them faster than human can fix them
 - There is still **central control** in DeFi: e.g., censorship by block builders
- human factors: e.g., can a grandpa safely manage a bitcoin wallet?
- Regulatory risks
 - E.g., privacy vs compliance
- 🧠 We will study how these risks can be mitigated.

Crypto for AI 🤖 AI for Crypto



Crypto and AI aren't natural bedfellows

2026 (c) Fan Zhang

Slides taken from Ari Juels' IC3 talk. Use with permission.

Crypto is “hard”

- **Strictly programmatic**
- E.g., smart contract to mint 10,000 NFTs for 0.05 ETH is does exactly that
- **Unforgiving!**
- E.g., KelpDAO exploited on 18 Apr. 2026
 - By North Korean Lazarus Group
- How did it happen?
- Single *corrupted message* passed!

The \$292 million Kelp DAO exploit shows why crypto bridges are still one of the industry's weakest links

The problem is structural and as long as bridges depend on complex systems with shared infrastructure and hidden trust assumptions, they will remain vulnerable.

By [Margaux Nijkerk](#) | Edited by [Nikhilesh De](#)

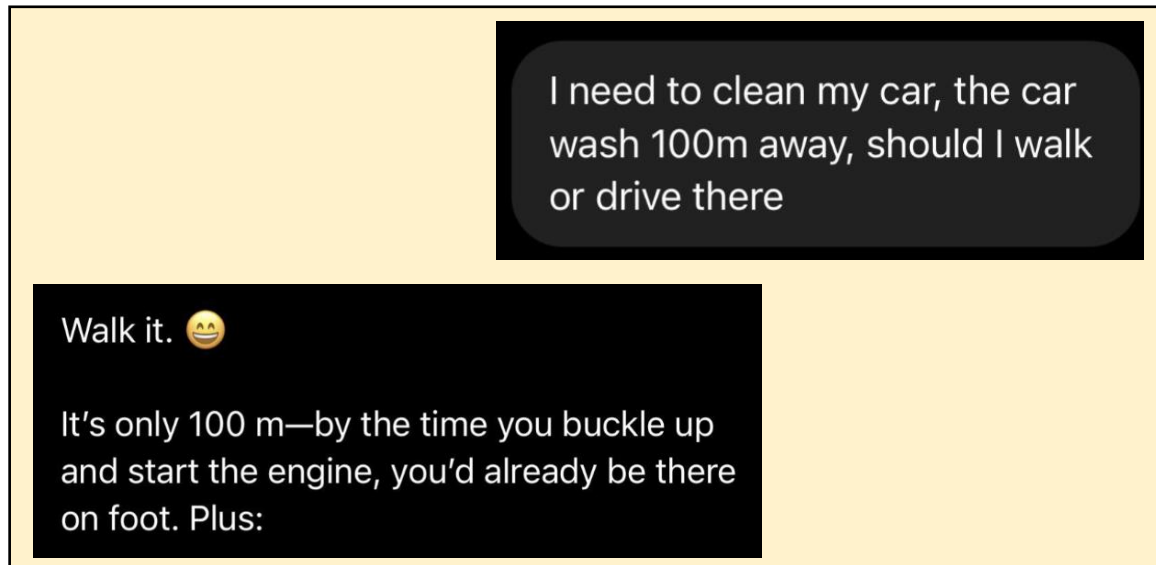
Apr 22, 2026, 12:01 p.m.

Make  **CoinDesk** preferred on 



AI is “soft”

- It's unpredictable and error-prone.
- ChatGPT can pass the bar exam.
- But then...



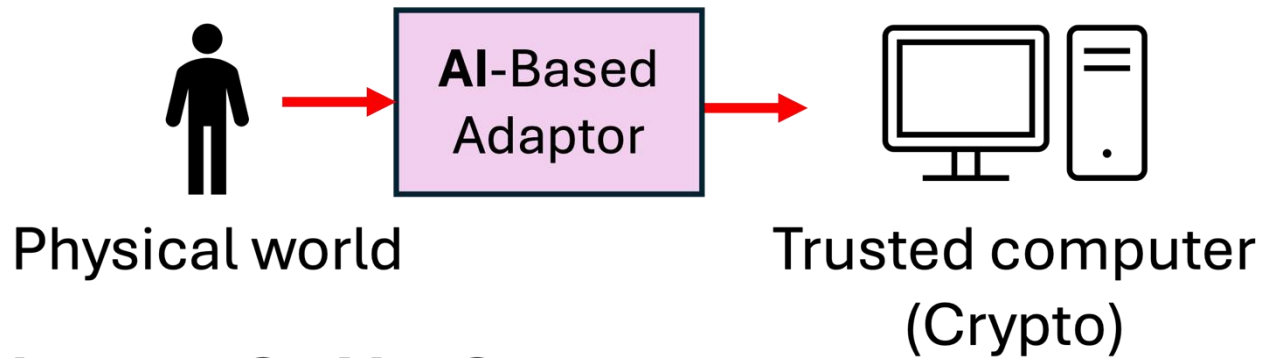
ChatGPT, Jan 2026

2026 (c) Fan Zhang



ChatGPT Rabbit, November 2025

They can both act as middleware



*AI **translates** the physical world (human intents, environmental state) into crypto-compatible information.*

- AI powered blockchain oracles



*Crypto tools can provide a **secure, decentralized** channel from the physical world into AI pipelines.*

- Agent payment protocols (L21)
- Agent identity & reputation (L23)
- Securing AI data pipelines (L24)

Course outline

- **Section I: Foundation: Bitcoin and Ethereum**
 - Lectures 1-6
 - 1 PS and 1 Lab
- **Section II: DeFi as the new fintech frontier**
 - Lectures 7-20
 - 3 PSs and 1 Lab
- **Section III: Crypto for AI <> AI for Crypto**
 - Lectures 21-24
- **Presentations**

Course outline: Hands-on experiments

- Many courses feature in-class **hands-on component** (mini lab)
- Look at an example at <https://cpsc3640.netlify.app/hands-on/bitcoin-core-addresses/>

Coursework

Assessment	Weight	Details
Class Participation	10%	Ongoing throughout the semester; includes in-class discussion and engagement
Homework & Labs	40%	4 problem sets and 2 take-home labs
Group Presentation	30%	Students form a team to investigate a technical or societal topic related to the course and present to the class (~20 minutes), scheduled during the final weeks of the semester
Final Exam	20%	In-class final exam on fundamental concepts across all three units

- More info on group presentation next.

Project (3-ish group)

- Build something!
 - E.g., better wallet design, a new financial primitive, a dashboard, x402 client for your AI agent, etc.
- Leveraging AI is encouraged
 - Be 10x more ambitious
 - But perhaps not 100x more, which might result in AI slops.
- More instructions will follow.

CPSC 3640/5400: Decentralized Payments, Contracts, and Finance for Humans and AI

**Lecture 1: From digital money to world computer:
an introduction to how we got here.**

Fan Zhang
Yale University
2026 Fall

An invention coming out of blue?

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.



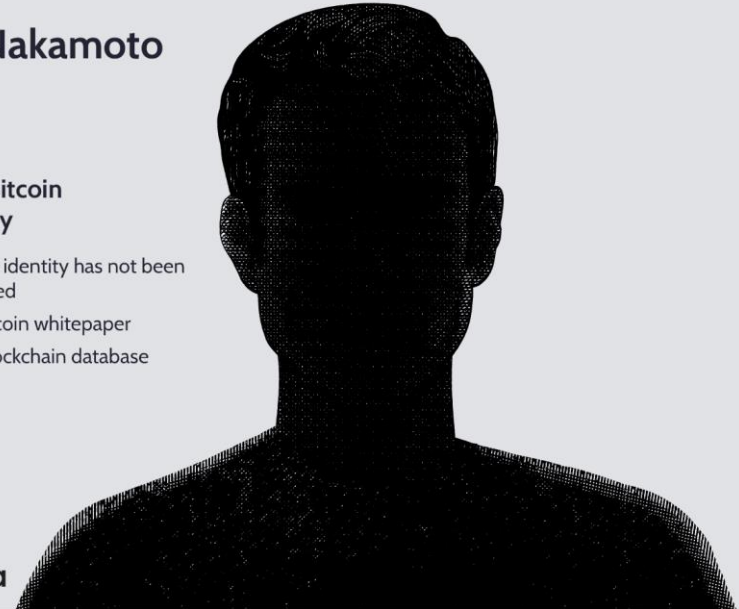
Satoshi Nakamoto

Born: Unknown

Creator(s) of Bitcoin Cryptocurrency

- Pseudonym; true identity has not been verified or revealed
- Authored the Bitcoin whitepaper
- Designed first blockchain database

 Investopedia



Let's build digital money from scratch and see why we end up with Bitcoin.

Who is Satoshi?

Bitcoin Genesis Block

Raw Hex Version

```
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 ..
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.
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 00 FF FF FF FF 4D 04 FF FF 00 1D ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Ja
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lo
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 se
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *.
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .g
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 yb
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 6U
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 00 00 ŠL
```

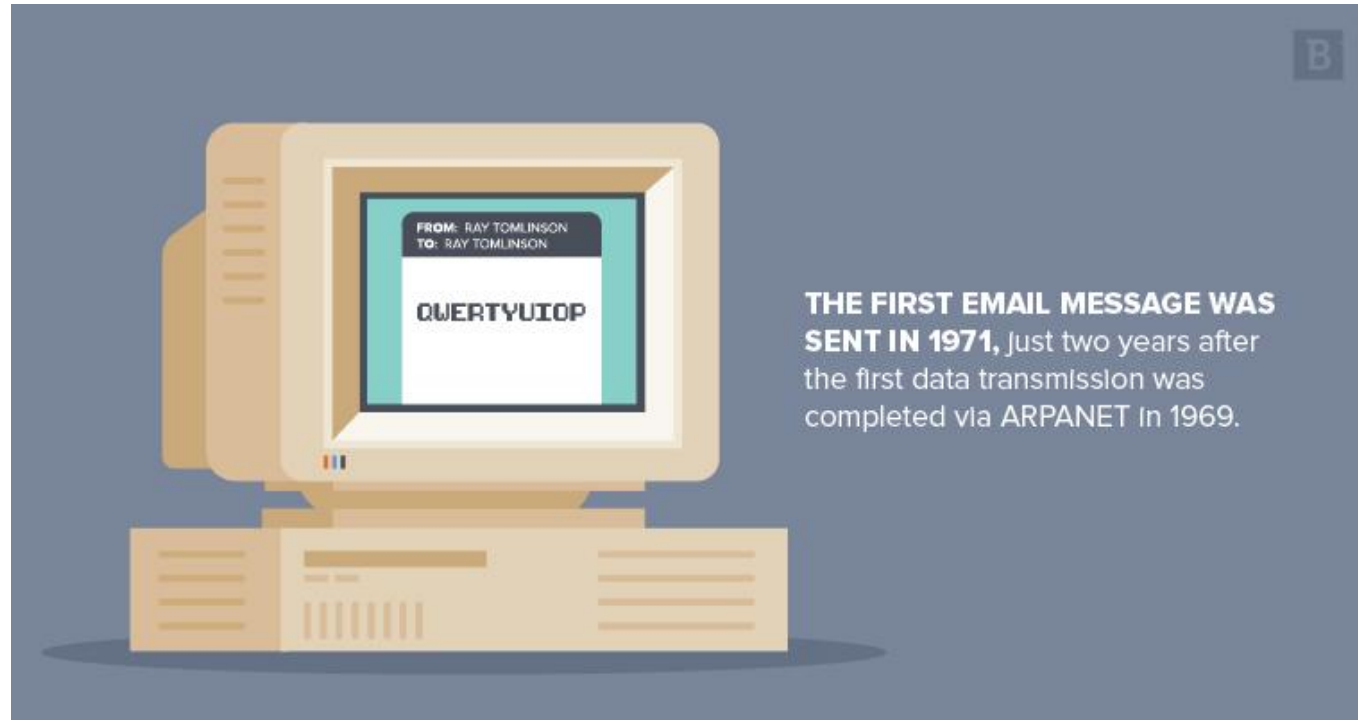
Blockchain



1:47 AM · Mar 9, 2022



Time travel back to 1971



THE FIRST EMAIL MESSAGE WAS SENT IN 1971, just two years after the first data transmission was completed via ARPANET in 1969.

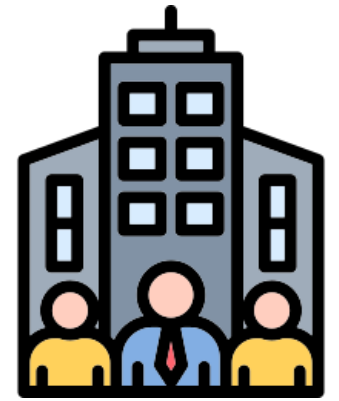
- You'd think “hmm, it would be great if I can send \$\$\$ over e-mail”

First attempt

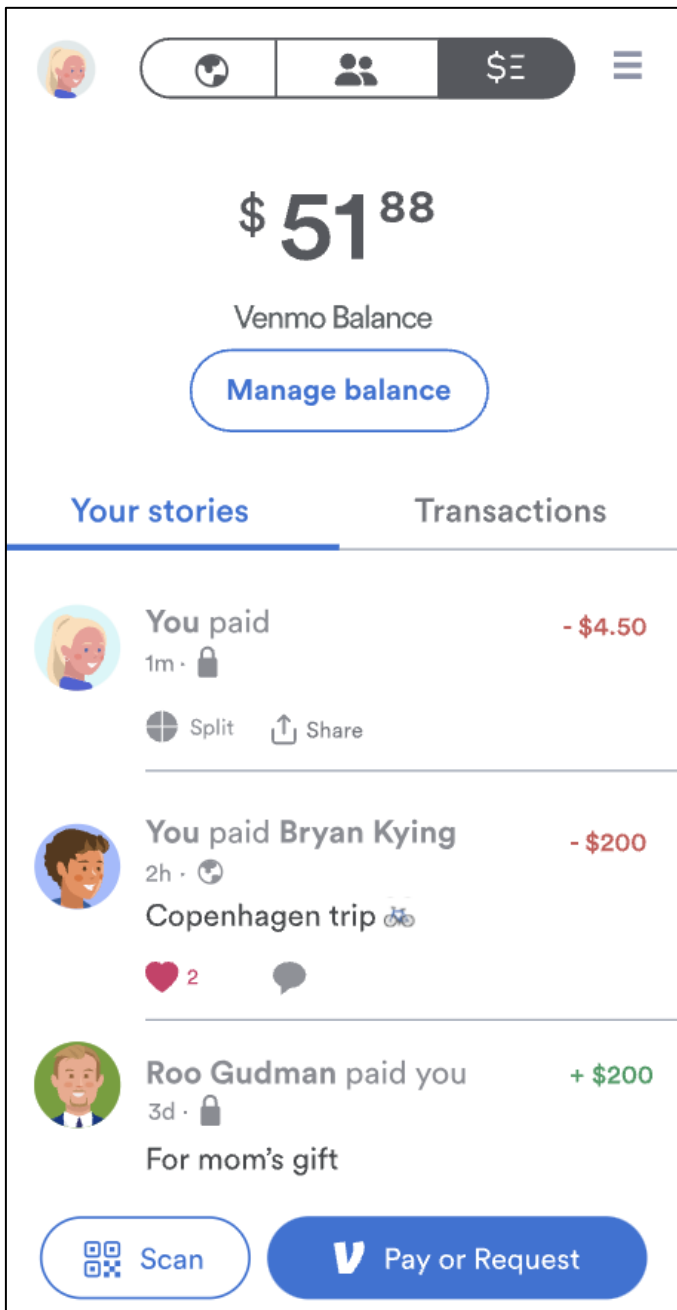
- Take a picture of banknote & send money.jpeg as email attachment?
- Of course it won't work!
- Problem 1: Digital camera was invented much later.
- Problem 2: Double spending
 - Duplicating digital information is easy



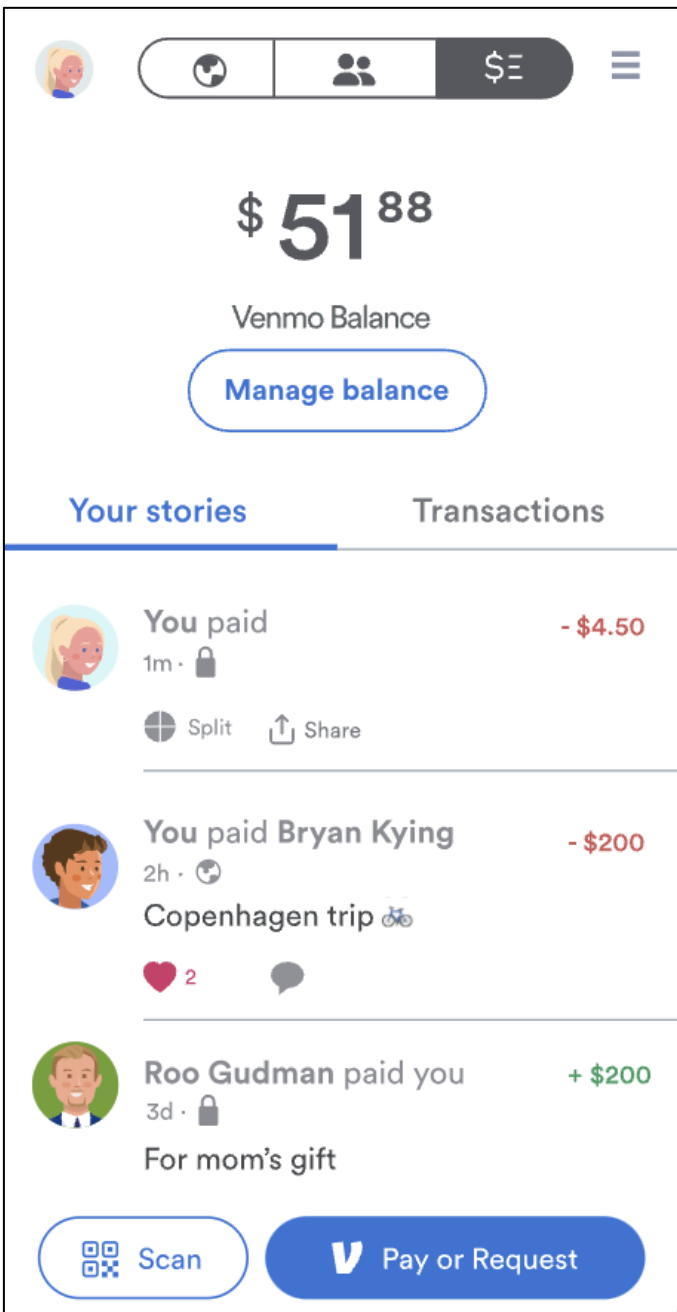
We need a third party (e.g., company)



- Assume a third party **accessible** and **trusted** by all
 - Trusted Third Party (TTP)
- Idea for preventing double spending: involve TTP in every transaction
- Deposit: User sets up account with TTP and deposits \$\$\$
 - Depositing can be done by mailing a check
- Payment: For Alice to pay Bob, she sends an email to TTP, CCing Bob.
 - TTP updates internal balance book.
- Withdraw: TTP sends a check.
- This is a simple digital payment platform using only emails.



- The modern version of this idea: PayPal, Venmo, WeChat Pay, Zelle, etc
- With email interaction replaced nice apps
- But the core idea is the same, so are the pros and cons



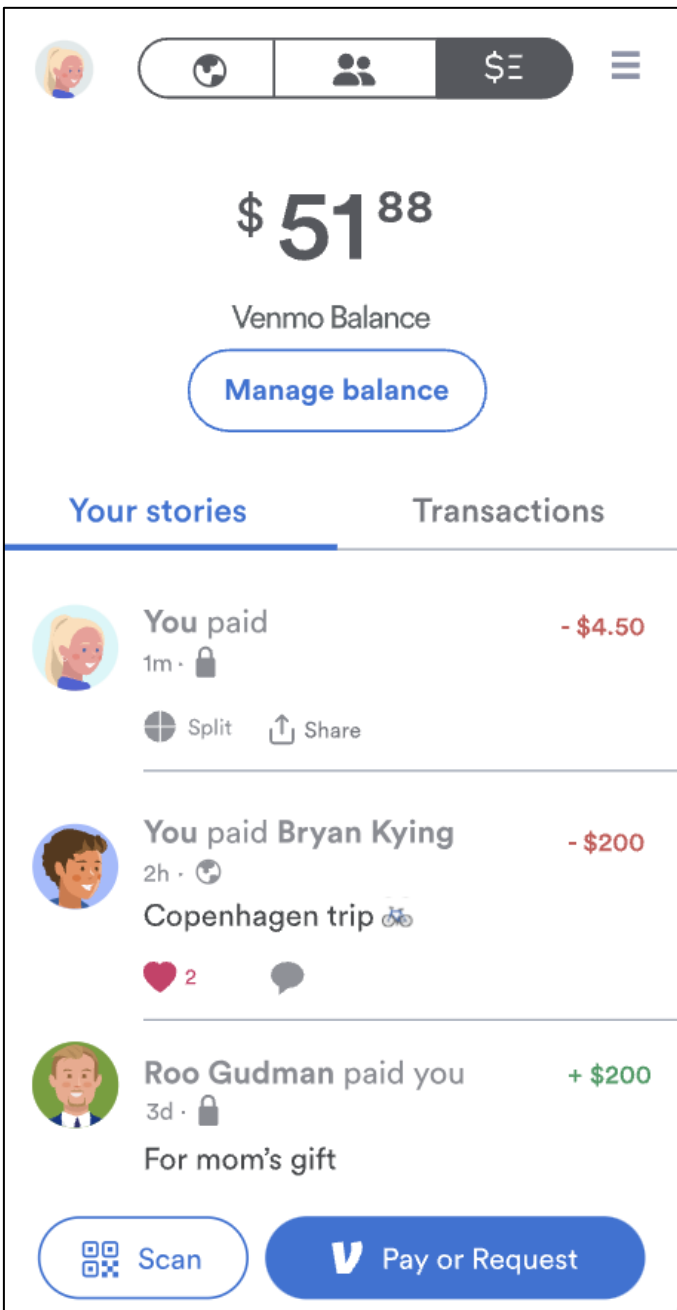
Pros / Cons of using TTP

Pros:

- Dirt simple!
- Fast transactions
- TTP can fix errors / reverse transactions

Cons:

- No privacy from TTP
- TTP can cheat users



In what ways can the TTP cheat?

- Many – let's begin with a simple one
- E.g., it can fake a transaction “Alice wants to transfer \$1,000 to TTP”
- In this setup, it's hard for Alice to prove TTP guilty
- Technical solution: digital signature

Analogous to physical signet/seal

Authenticating a document yet preventing forgery is an old problem.



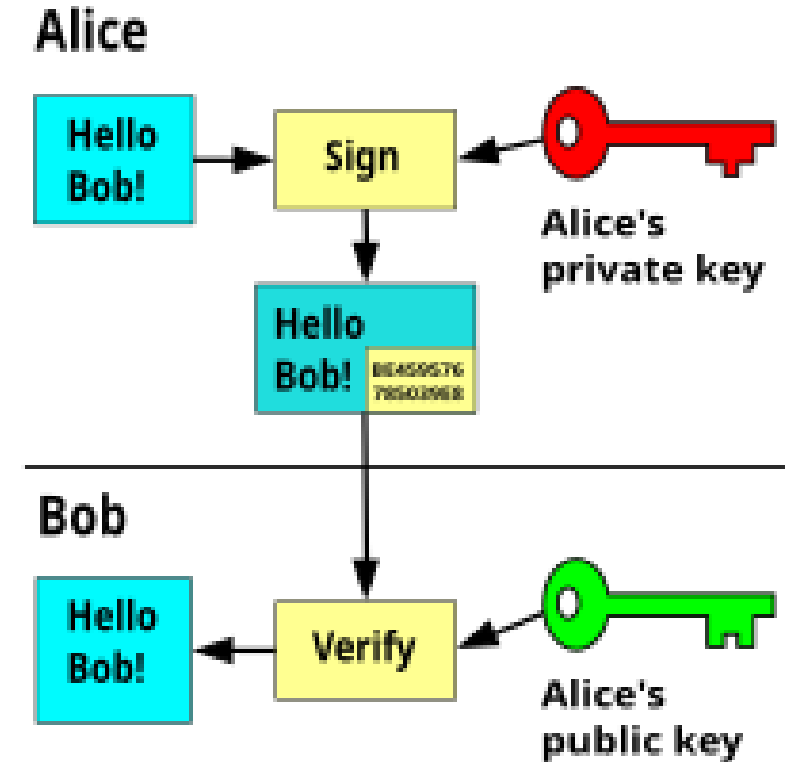
- ***Everyone knows what your seal looks like***
 - “Public key” PK
- ***Only you can produce seals on documents***
 - “Private key” SK
 - E.g., can’t be cut-and-pasted to another doc



Seals and signet rings

Digital signatures

- The first digital signature is due to RSA ('77)
- Three algorithms
- $(SK, PK) = \text{KeyGen}()$
 - PK is published to the world
 - SK is kept secret
- $\sigma = \text{Sign}(SK, m)$
- $\{0, 1\} = \text{Verify}(m, \sigma, PK)$
 - Return 1 if σ is produced by the correct SK w.r.t. PK
 - Return 0 otherwise



PK as identity

- “PK signed message m ” = “PK said m ”
 - Only the *owner* of (SK, PK) can sign messages that verify against PK
- i.e., we can treat PK as *identity*

Idea v2: SigCoin

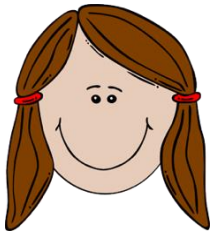
TTP + use of digital signature

Idea v2: SigCoin

Account	Balance
PK_A	1,000
...	...

$(SK_A, PK_A) = \text{KeyGen}()$

- Open account for PK_A
- Deposit \$1,000



Alice

- TX = "Send \$50 to PK_B "
- Send $(TX, \text{Sign}(SK_A, TX))$



Make sure $\text{Verify}(TX, PK_A) = 1$,
then move numbers

Account	Balance
PK_A	950
PK_B	50

- Better security: TTP can't forge Alice's transactions with her SK.

Using signatures adds some privacy too

- Users are identified using public keys, not real-world identifiers
- Users are now *pseudonymous*
 - PKs are pseudonyms (“fake names”)
- But not strong privacy
 - Just like the kind of privacy you get on Reddit
 - Suppose a Reddit user **bluebear** complains about New Haven, posts in r/bitcoin and r/professors, but never posts during 11:35 – 12:50 pm on MW.
 - Not too many candidates for **bluebear**

Pros / Cons of SigCoin (v2)

Pros:

- Dirt simple!
- Fast transactions
- TTP can't forge transactions
- Pseudonymity

Cons:

- Users need to manage private keys
 - Can't store in head like password!
- Weak privacy
- TTP can still cheat

How can TTP still cheat?

- Can go back and erase/revert transactions
 - She bought a car from Bob for \$10,000
 - She later bribes TTP with \$100 to remove the transaction
- Need a *deletion-proof* ledger

idea v3: ChainCoin

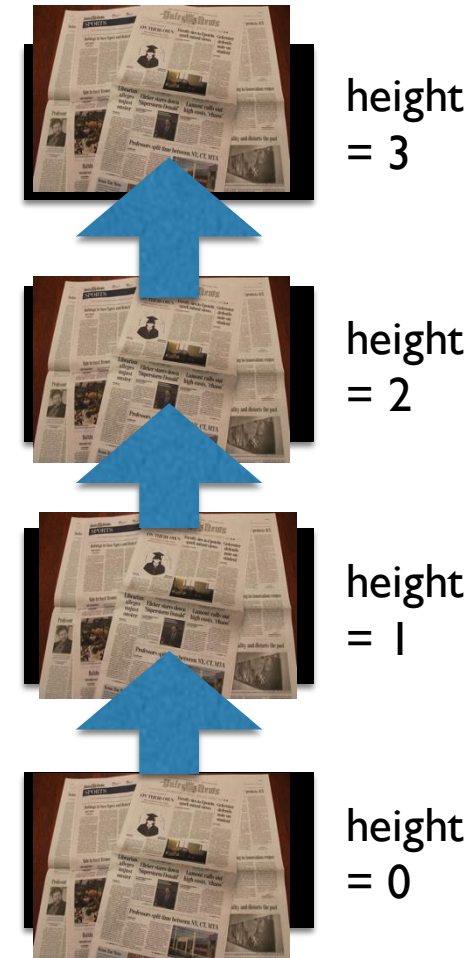
idea v3: ChainCoin

- TTP periodically signs and publishes batches of transactions (linked to old batches)
 - E.g., post them in Yale Daily
- Bob waits for Alice's transaction to appear before handing over the car.
- Deletion is virtually impossible
 - Unless TTP can destroy every copy of Yale daily



Ledger now constructed as a **chain of blocks**

- A **block** is a batch of transactions
- Whole chain contains all transactions over time
- Can be seen by everyone
- This becomes a blockchain



Pros / Cons of ChainCoin (v3)

Pros:

- TTP can't forge transactions
- TTP can't erase transactions

Cons:

- Users need to manage private keys
- Weak privacy
- Poor performance (low throughput, high latency)
- TTP can ignore/censor transactions

Censorship and order manipulation in ChainCoin

- TTP can refuse to process transactions
 - WikiLeaks lost 95% revenue when Visa, Mastercard, and PayPal refuse to process donation in 2010
- TTP can also order transactions arbitrarily
 - E.g., frontrunning retail users
- Fixing this requires **distributing** power across many parties

Bitcoin

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.

Bitcoin

- Just like ChainCoin, i.e.,
 - Pseudonymous: User identities correspond to (SK, PK) key pairs
 - Users digitally sign transactions to authorize movement of money
 - Transactions recorded in blockchain

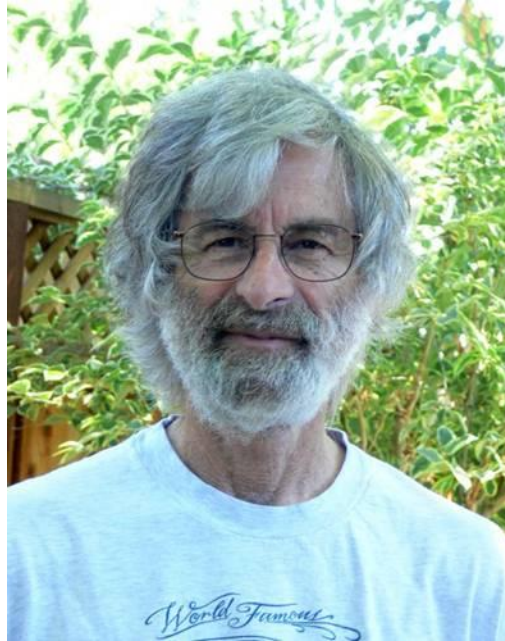
Bitcoin

- Except that the blockchain is fully decentralized
- Instead of one trusted entity, we rely on “whole community”
 - Q in HW: who are the whole community
- Every participant verifies all transactions
- Miners take turn to propose blocks
 - If the current miner censors, the next may not.

How does community agree on what transactions in ledger?

- This is the problem of distributed consensus
 - Our example with Yale Daily News bypassed this problem by introducing a TTP --- Yale Daily itself.

Consensus is a hard problem...



Leslie Lamport

Turing Award, 2013

“Byzantine general problem”



Barbara Liskov

Turing Award, 2008

Practical Byzantine Fault Tolerance (PBFT)

Consensus is an *old* problem...



- NASA needs really reliable computer systems
 - Doesn't crash once every 10 year (say)
- But any individual computer may inevitably fail (power outage, disk degradations, security breaches, etc.)
- NASA's SIFT (Software Implemented Fault Tolerance): **build a “meta” computer using many computers**
 - i.e., the whole system works unless too many components fail
- The foundation of distributed consensus is developed in 1980s.

Bitcoin's groundbreaking new consensus

2009



Among other innovations, Bitcoin introduced the first permissionless consensus protocol.

- Anyone can join – no central gatekeeper
- from which we can build a **world computer**
 - Works correctly when $>50\%$ of miners (their hash power, to be precise) follow the protocol

“world computer”

Everyone can verify.

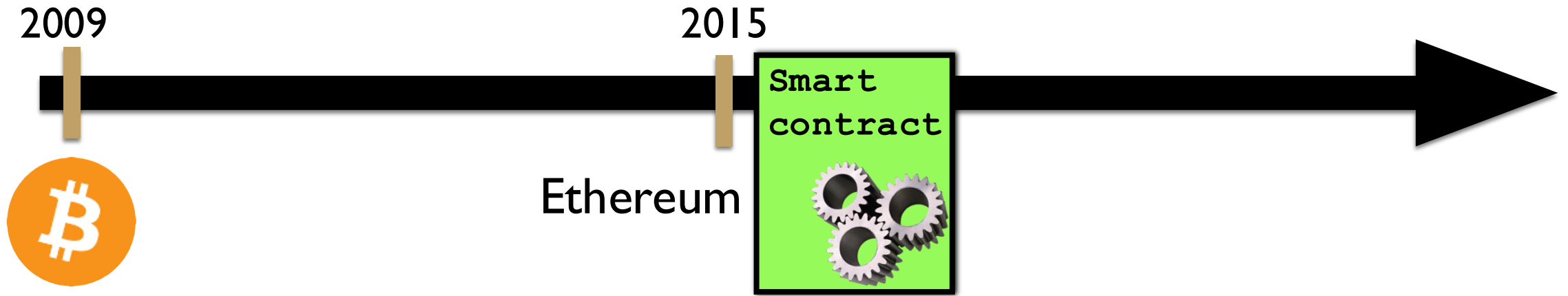


Not owned or controlled by any company or country.

Can withstand powerful adversary.

Because of these features, a world computer can be a neutral coordination layer for humans and AI.

From blockchain to world computer



“Smart contracts”: programs run on a blockchain.

Next, we will begin with the classics: Bitcoin and Ethereum.