The final reflection assignment is now posted on the course website. It is due 11:59pm (Pacific Time) on March 16th and should be turned in via Gradescope.
The trust machine

The technology behind bitcoin could transform how the economy works

Thanks to Dan Boneh for idea behind the animation
Possible Applications of Blockchain

- Payment system for unbanked populations
  - Potential hedge against inflation for some currencies
- Supply chain/inventory management
  - Tracking goods in supply chain
- Insurance
  - Smart contracts for reporting claims and compliance
- Healthcare
  - Tracking anonymized patient data
- Real estate
  - Ownership records and verification
- Identity management
  - Verification of citizenship, birth records, drivers license, etc.
- Voting
  - Verifiable record of voting with identity verification
2 Questions I Am Asking

1. What problem are we trying to solve?
2. What are the benefits and costs of solving it in a decentralized way as compared to the alternative?
A Favorite Use Case: Cryptocurrency

Images: Public Domain
Catching On?

Overall cryptocurrency market capitalization per week from July 2010 to March 2023 (in billion U.S. dollars)

Sources:
CoinGecko; BitInfoCharts
© Statista 2023

Additional information:
Worldwide; July 2010 to March 2023; Note that due to changing exchange rates, the USD value applies in retrospect
Catching On?

OVER 420+ MILLION CRYPTO OWNERS WORLDWIDE

- Singapore-backed blockchain firm TripleA estimates that as of 2022, there are over 420 million crypto users worldwide

“The blockchain technology that underlies Bitcoin is a major technical breakthrough that could, in time, revolutionize both the Internet and the financial industry as we know them—and the first steps of that potential revolution are now under way.”

— Jon Evans, TechCrunch columnist

“Bitcoin is better than currency in that you don’t have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient. [...] The Bitcoin technology is key.”

— Bill Gates

**What Problem Are They Solving?**

Figure 1. Shares of people who report having very high or high trust in each of the four institutions. *Notes:* The vertical lines delineate the periods of two crucial events: the subprime crisis (August 2007) and the bankruptcy of Lehman Brothers (September 2008).

“The crash of 2008 revealed most of what we know about Wall Street’s confidence game at the time. It entailed a vast manipulation of ledgers. **The recorded value of the assets those ledgers were supposed to track—including those havoc-causing credit default swaps—turned out to be largely vapor.** The shock of Lehman wasn’t so much that it happened, but that even most experts trusted the ledgers so completely until it was too late. [...] **The real problem was never really about liquidity, or a breakdown of the market. It was a failure of trust.** When that trust was broken, the impact on society—including on our divided political culture—was devastating.” — *The Truth Machine*

What Problem Are They Solving?

“On October 31, 2008, while the world was drowning in the financial crisis, a little-noticed “white paper” was released by somebody using the pen name “Satoshi Nakamoto,” and describing something called “Bitcoin,” an electronic version of cash that didn’t need state backing. At the heart of Nakamoto’s electronic cash was a public ledger that could be viewed by anybody but was virtually impossible to alter. This ledger was essentially a digitized, objective rendering of the truth, and in the years to follow it would come to be called the blockchain.”
— The Truth Machine

ALLOCATING YOUR MONEY?

I want you to think about the year after you graduate from Stanford. You are earning real money for the first time. If you want to protect it and enable it to grow in value, what do you do with it? Why?

Investment Portfolio

- Savings/checking account
- Stocks
- Bonds
- Mutual funds
- Gold/other commodities
- Cryptocurrency
- Under your bed
How Do Others Weigh The Risks?

16% of Americans say they have invested in, traded or used a cryptocurrency; a plurality of them say their investments have done worse than expected

% of U.S. adults who say the following

- **16%** have ever invested in, traded or used a cryptocurrency such as bitcoin or ether
- **71%** have not invested in, traded or used cryptocurrency, but have heard at least a little about it
- **12%** have heard nothing at all about cryptocurrency*

Among this group, % who say thinking about the money they have invested in cryptocurrency, their investments have done

<table>
<thead>
<tr>
<th>Overall</th>
<th>Better than they expected</th>
<th>About the same as they expected</th>
<th>Worse than they expected</th>
<th>Not sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>15</td>
<td>31</td>
<td>46</td>
<td>8</td>
</tr>
</tbody>
</table>

*The question about investing in, trading or using cryptocurrency was asked of those who had heard at least a little about cryptocurrency, but is presented here as among all adults. The 12% of U.S. adults who said they have heard nothing at all and the 1% who gave no answer on that item did not receive the follow-up question.

Note: Those who did not give an answer or who gave other responses are not shown.

Source: Survey of U.S. adults conducted July 5-17, 2022.

Who’s In? Who’s Out?

Why Americans haven't been convinced on cryptocurrency

August 30, 2022 · 5:10 AM ET
Heard on Morning Edition

FADEL: Thank you so much for being here. So 16% of American adults say they've invested, traded or used crypto. What's keeping Americans from investing more in cryptocurrency?

MESIDOR: Well, let's face it. If the traditional financial system has worked for you, if you've benefited from traditional markets, you are probably cool to crypto. That's why we've seen Black and Latino communities lead adoption. But the blitz that occurred, right - the Super Bowl ads, all of the media - it happened around the time that a recession was looming. Traditional markets were going into a bear market. So I think it's just timing. I think, you know, every American right now, regardless of what their portfolio includes, their portfolio does not look good. They're not happy. So it's not crypto. Crypto is not happening in isolation.

Source: https://www.npr.org/2022/08/30/1120023698/why-americans-havent-been-convinced-on-cryptocurrency
What Are the Returns?

Bitcoin Price

Image: Wikideas1, Wikimedia, Public Domain
What Are the Returns?

Ethereum Price

Image: Wikideas1, Wikimedia, Public Domain
What Are the Risks?

**Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities**

The world’s biggest cryptocurrency exchange confirmed that assets were stolen from the Binance Smart Chain network, the latest in a series of attacks on so-called cross-chain bridges.

By Ephrat Livni  
Oct. 7, 2022
What Are the Risks?

Binance, the world’s biggest cryptocurrency exchange, confirmed on Friday that $570 million had been stolen in a hack of a blockchain it runs that serves as a bridge for asset transfers between networks. The attack on the Binance Smart Chain network highlighted weaknesses in decentralized finance, or DeFi, where transactions are controlled by code.

“Software code is never bug free,” Binance’s chief executive, Changpeng Zhao, said in an interview with CNBC. He emphasized that no users had lost money in the hack but said that so-called cross-chain bridges were particularly vulnerable to hacks and the industry needed to get better at learning from them.

Crypto-focused bank Silvergate is shutting operations and liquidating after market meltdown

Published Wed, Mar 8 2023-4:35 PM EST | UPDATED 4 HOURS AGO

MacKenzie Sigalos
@KENZIESIGALOS

Key Points

- Silvergate Capital announced on Wednesday that it will wind down operations and liquidate its bank.

- The firm has served as one of two main banks for the crypto industry, along with Signature Bank.

- All deposits will be fully repaid, according to a liquidation plan shared on Wednesday.

How Do We Weigh the Risks?

Are these problems inherent to blockchain and decentralized finance?

Or are they a function of intermediaries that have grown up around blockchain and decentralized finance?

It’s hard to figure out. So let’s go back to the beginning...
Today’s Agenda

1. What are new models of finance and how are they different?
2. What do the enthusiasts of cryptocurrency want to achieve?
3. What new problems are created or old problems become unsolved when we decentralize?
5. How is government approaching the regulation of decentralized finance?
What is Money For?

Money is:

- A medium of exchange
- A store of value
- A unit of account (that enables us to set prices)
- An alternative to bartering

Source: Wikimedia Commons; Wikipedia
Where Do Banks Come From?

• Since at least Ancient Rome, a vital function of banks has been functioning as currency exchanges
• Modern banking arose in Renaissance Italy
• Banks take your money in the form of *deposits* — they pay you an interest rate for storing it there
• Banks lend money in the form of *loans* (usually with fixed terms)—they charge a higher interest rate for borrowing it

Source: World History Encyclopedia; Posterazzi
From Banking to Stock Markets

• Public companies list some of their shares (part of the company stock, or parts of the equity of the company) on the stock market; first stock exchange is 1609 in Amsterdam
• You can buy shares of the companies, and they will either increase or decrease in value
• You can mix and match companies in funds (such as mutual funds and exchange-traded funds) and buy those too
Central banks are created, beginning in the mid 1600s

- Developed in order to control economic shocks and promote economic prosperity
- With supervisorial and regulatory power, monopoly control over the monetary base
- Use indirect mechanisms (e.g., interest rates, reserve requirements, printing of money) to control the money supply
- Run by “experts”, meant to be free of politics
- Their existence remains questioned even today
“The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”

"As a new form of money that is not tied to any government or bank, Bitcoin represents a revolutionary step forward in the evolution of financial systems.”

— Satoshi Nakamoto
A Declaration of the Independence of Cyberspace

by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel,
I come from Cyberspace, the new home of Mind. On behalf of the future, I
ask you of the past to leave us alone. You are not welcome among us. You

“From the beginning, Bitcoin presented itself in the garb of a transformative utopian project, with roots in cypher-punk, anarchist, and libertarian promises of technology. **Robbing governments and banks of their ability to control money would create on this view a world in which states had lost control over tax revenue and credit creation, thereby left unable to finance wars.**”

— Stefan Eich

Jack Dorsey hopes bitcoin will help bring about world peace

“My hope is that it creates world peace or helps create world peace,” Dorsey said during a “The B Word” webinar on Wednesday.
“Cryptoeconomy > Fiat Economy. [...] All manner of financial instruments, corporate vehicles, accounting, payroll, and the like can be done on-chain outside the control of states.” — Balaji Srinivasan, *The Network State*
<table>
<thead>
<tr>
<th>Traditional Finance</th>
<th>Decentralized Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Controlled by a small number of institutions</td>
<td>Not controlled by a small set of institutions (debatable)</td>
</tr>
<tr>
<td>Requires trust in a financial institution (and its trust in you, generally speaking)</td>
<td>Requires less (or even no) trust</td>
</tr>
<tr>
<td>Less accessible (unbanked populations)</td>
<td>More accessible (doesn’t require a relationship with a financial institution)</td>
</tr>
<tr>
<td>Well-established (existing legal framework, deposit insurance, more widely accepted, etc.)</td>
<td>Very new (no full legal framework, no deposit insurance, not as accepted by wider society)</td>
</tr>
<tr>
<td>Fraud Protection</td>
<td>No inherent fraud protection (would require centralization)</td>
</tr>
<tr>
<td>Government Oversight</td>
<td>Less government oversight (though that’s changing)</td>
</tr>
</tbody>
</table>

What is Cryptocurrency?

Cryptocurrencies enable people to send and receive money over the internet without needing to involve a central authority, such as a bank or an application (PayPal or Venmo). Bitcoin was the first, and there are now 10,000+ cryptocurrencies in existence.
How Does Blockchain Help?

- If you have a (decentralized) ledger, you can keep track of tokens that can be exchanged
  - Maintain a record of transaction between entities to determine how many tokens each person has
    - Recall, this is how your bank balance is maintained
  - But rather than a government issuing tokens (e.g., dollars), you create your own token that can be exchanged
    - If there is a limited number of tokens available (scarcity), people may ascribe value to it
    - If value is ascribed to it, it can be exchange for other things of value, essentially acting as a currency
- Cryptocurrencies are just tokens that are kept track of on distributed ledgers that people ascribe value to
  - Generally, there is a mechanism for limiting the supply of tokens
    - E.g., Bitcoin is limited to 21M tokens
Are Intermediaries Displaced?

Yes. This is disruptive to traditional finance institutions (e.g. commercial banks, central banks, investment banks, brokerage firms, etc.). In some ways, they cut out the “middlemen”.

No. Cryptocurrencies are not fully “trustless”. They depend on all sorts of intermediaries from exchanges to crypto-lending platforms. They require interaction with traditional financial institutions so digital currencies can be exchanged for other currencies. They also require software developers, miners, validators, etc. to make the decentralized technical systems work.
1. What are new models of finance and how are they different?
2. What do the enthusiasts of cryptocurrency want to achieve?
3. What new problems are created or old problems become unsolved when we decentralize?
5. How is government approaching the regulation of decentralized finance?
The Most Ambitious: Hayek
“I do not think it an exaggeration to say that history is largely a history of inflation, and usually of inflations engineered by governments and for the gain of governments. [...] Our only hope for a stable money is indeed now to find a way to protect money from politics.”
“The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”

"As a new form of money that is not tied to any government or bank, Bitcoin represents a revolutionary step forward in the evolution of financial systems.”

— Satoshi Nakamoto
What Problem Was Hayek Solving?
What Problem Was Hayek Solving?

U.S. Inflation Rate

Image: Public Domain, adapted by adding a circle
What Problem Was Hayek Solving?

- Hayek writing during a time of great inflation (sound familiar?)
- The ultimate aim of our currency system should be price stability.
- Politics is the cause of most inflation
- Governments feel pressure to take short-term actions that inflate the currency. Why?
- In order to alleviate economic pain in the short-term (e.g., unemployment) and help keep their approval up/keep them in power
- But, in the long-term, these actions cause inflation to increase and harm the economy as a result
- So, depoliticize currency! Get the government out of it!
“Money is power. This simple truth is valid for national and international relations. Those who wield power control money. Those who manage and control money wield power. An international monetary system is both a function and an instrument of prevailing power structures.”

What Problem Were They Solving?

- The politics of money are not just national, but international
- Different nations have different levels of power depending on their currency
- Therefore, the best thing we can do is to create an international, democratic system to regulate currency
- The IMF is not that structure — “Although the Third World counted close to one hundred countries that included more than two-thirds of the world’s population, its cumulative voting share at the IMF amounted to no more than 35% and thus less than the 40% of the five leading industrial powers alone.”

What Problem Were They Solving?

The proposal for a new, international monetary system:

- Democratic management and control
- Universality (all countries participate)
- The establishment of an international currency unit
- Automaticity in transfer of resources
- A new international monetary authority

Annex

THE ARUSHA INITIATIVE:

A CALL FOR A UNITED NATIONS CONFERENCE ON INTERNATIONAL MONEY AND FINANCE *

A More Modest Ambition

OK maybe digital currencies won’t replace national currencies anytime soon...

What do they offer us?

• Medium of exchange with different properties
• Asset that can store value and increase in value
• A part of a diversified financial system
1. What are new models of finance and how are they different?
2. What do the enthusiasts of cryptocurrency want to achieve?
3. What new problems are created or old problems become unsolved when we decentralize?
5. How is government approaching the regulation of decentralized finance?
## Recall the Value of Centralization

### Benefits
- Creates order and legitimate authority
- Can facilitate cooperation
- Can punish transgressors, handle adversaries

### Costs
- Can erode individual freedom
- Increases fragility
- Compromises stability over time
Intermediaries to Solve Problems

- Protect the value of people’s assets
- Curb risky behavior by banking institutions
- Prevent consumer fraud
- Facilitate investment of capital
- Prevent securities fraud
- Ensure that financial system is not a safe harbor for ill-gotten gains
- Prevent organized crime and international terrorism
- Attract capital to the U.S. financial system
- Maintain control over the money supply

THANK YOU to commercial banks, central banks, brokerages, investment bankers, and government regulation(!), etc.
What Are the Conseq. of Disruption?

Source: Public Domain
Strategic actors are going to use these new technologies to their benefit. This includes criminals who will (1) use cryptocurrency to facilitate the commission of crimes or to support terrorist activity (2) hide financial activity, such as through money laundering or sanctions evasion and (3) commit crimes within the crypto currency market itself.

Bitcoin was the currency of the Silk Road website – the most sophisticated criminal marketplace on the internet in 2013.

A new threat is “Ransomware-as-a-service” where developers license ransomware tools to affiliates, in exchange for payments. Cryptocurrencies are a key tool facilitating this criminal enterprise.
“If there is one point we want to make to the Members of the Banking Committee, it is that the transparency of blockchains enhances the ability of policymakers and law enforcement to detect, disrupt, and ultimately, deter illicit activity.”

-- Jonathan Levin, Co-Founder, Chainalysis
FIGURE 2: WEEKLY COUNT OF VIRTUAL CURRENCY COMPLAINTS AND BITCOIN PRICE, OCT. 2018 TO SEPT. 2022

What are the major issues?

1. Fraud, theft, hacks, and scams
2. Difficulties making timely, efficient transactions
3. Customer service concerns
4. Frozen accounts and platform bankruptcies
5. Crypto-asset card complaints
Crypto Could Threaten Financial System, Federal Risk Panel Warns

Regulators’ report in response to President Biden’s order highlights cryptocurrency vulnerabilities

“The financial stability risks of crypto-assets would be substantial if those vulnerabilities were to remain in place while the scale of crypto-asset activities and interconnectedness with the traditional financial system were to grow rapidly,” the risk panel said in a 120-page report.
What are the main risks?

1. Interconnectedness that quickly spreads losses across the crypto market and can spill into traditional finance institutions
2. Very high and excessive amounts of leverage ("borrowed money") that can exacerbate shocks to the industry
3. Prevalence of fraud and market manipulation, in highly unregulated space
Cyber Vulnerability

Total number of thefts and value stolen by type of victim, 2015 - 2022 Q1

Almost 97% of all cryptocurrency stolen in the first three months of 2022 has been taken from DeFi protocols, up from 72% in 2021 and just 30% in 2020.

How? Criminals are exploiting “open source” to identify and exploit vulnerabilities in the code.
The dollar’s role as the primary reserve currency for the global economy allows the United States to borrow money more easily and impose painful financial sanctions. But some experts say the costs to areas such as the Rust Belt are too high to bear.
Today’s Agenda

1. What are new models of finance and how are they different?
2. What do the enthusiasts of cryptocurrency want to achieve?
3. What new problems are created or old problems become unsolved when we decentralize?
5. How is government approaching the regulation of decentralized finance?
SBF: The Villain

Images: Public Domain; Cointelegraph, Wikimedia (CC-BY 3.0)
SBF: The Villain

- May-July 2022: Terra-Luna (stablecoin) collapses trigger a wave of bankruptcies among crypto lenders. FTX bails a number of these out.
- Nov. 2, 2022: Leaked financials from Alameda show that much of Alameda’s holdings are in FTX’s native token, FTT.
- Nov. 6, 2022: Binance announces it will sell off a lot of FTT. Alameda immediately announces that it will buy the FTT at $22.
- Nov. 8, 2022: Price of FTT craters to $6. Binance signs a nonbinding LOI to bail out FTX by buying a portion of it.
- Nov. 9, 2022: Reports come out that federal agencies are investigating FTX. Binance pulls out of deal after doing corporate due diligence on FTX.
- Nov. 10, 2022: Alameda Research shuts down, regulators in Bahamas freeze FTX assets.
- Nov. 11, 2022: Alameda, FTX, FTX.us, and lots of subsidiaries all file for bankruptcy. SBF resigns.

What Was FTX?

- FTX was a **cryptocurrency exchange** (also allowed for purchase and selling of other products, like NFTs)
- A cryptocurrency exchange is a centralized platform on which people can buy, sell, and exercise options on cryptocurrency
What Went Wrong?

The allegations against SBF include:

- Defrauding investors in FTX
- Money laundering
- Co-mingling of funds (taking FTX customer deposits and using them for non-approved purposes at FTX and Alameda)
- Conspiracy to do the above with other FTX leaders
- Operating an unlicensed money transmitting business
- Breaking campaign finance regulations
- And more...
Was This About DeFi?

Some say “No!”. This is just regular, old financial fraud.

- An intentional act by a bad actor — possible in any financial space, including TradFi
- e.g. Enron, Madoff, etc.
- Too much centralization was the problem (e.g. exchanges)

But:

- There would have been no FTX without the crypto bubble
- FTX was creating assets out of thin air to fuel its trades (e.g. FTT)
- The value of crypto depends on the existence of these unregulated intermediaries (e.g. exchanges open access to investors)

Today’s Agenda

1. What are new models of finance and how are they different? What do the enthusiasts of cryptocurrency want to achieve?
2. What new problems are created or old problems become unsolved when we decentralize?
4. How is government approaching the regulation of decentralized finance?
Nayib Bukele, President of El Salvador, made Bitcoin become legal tender.

Government-run “Chivo” app in which citizens could store bitcoin.

There was not widespread adoption.
China’s Ban

- After banning a number of aspects of crypto over the years (e.g., initial coin offerings in 2017), China fully banned crypto mining and trading in May 2021
- Some analysts speculate this is because China fears cryptocurrency continuing to facilitate capital flight from its markets
- In essence, crypto undermines the state’s control of currency

Roose’s Argument

In the early 2010s, the most common knock on social media apps like Facebook and Twitter was that they just wouldn’t work as businesses. Pundits predicted that users would eventually tire of their friends’ vacation photos, that advertisers would flee and that the whole social media industry would collapse. The theory wasn’t so much that social media was dangerous or bad; just that it was boring and corny, a hype-driven fad that would disappear as quickly as it had arrived.

What nobody was asking back then — at least not loudly — were questions like: What if social media is actually insanely successful? What kind of regulations would need to exist in a world where Facebook and Twitter were the dominant communication platforms? How should tech companies with billions of users weigh the trade-offs between free speech and safety? What product features could prevent online hate and misinformation from cascading into offline violence?

By the middle of the decade, when it was clear that these were urgent questions, it was too late. The platform mechanics and ad-
“Bitcoin’s colourful paeans to decentralization, competition, and efficiency stand in stark contrast to its actual workings. Instead of a decentralized, efficient currency, Bitcoin is today mostly a speculative asset with few if any uses as currency but a substantial energy footprint generated by an oligopolistic set of miners. Second, even in as far as Bitcoin succeeds in privatizing money (or in particular if it were to succeed more generally), this would amount to a de-democratization of an essential public good. It is not clear why any regulatory authority or democratically legitimated body should accept such a proposal.”
— Stefan Eich
1. Protecting consumers, investors, and businesses via monitoring and enforcement actions
2. Promoting access to safe, affordable financial services to address the fact that traditional finance leaves many behind
3. Fostering financial stability by helping financial institutions identify and mitigate cyber vulnerabilities
4. Reinforcing global financial leadership and competitiveness including in standard-setting bodies
5. Fighting illicit finance possibly by seeking legislation to close gaps in frameworks on unlicensed money transmitting
6. Exploring a Central Bank digital currency to enable a more efficient payment system and maintain the U.S. global position
Legislative Agenda in Congress

Warren wants a “comprehensive bill” focuses on consumer protection, anti-money laundering, and climate safeguards for crypto mining and which empowers the SEC

Stabenow’s bi-partisan bill – drafted in close consultation with FTX – uses the CFTC to set uniform standards for digital commodity platforms
What Makes This Hard?

Unclear who has authority and mandate to regulate.

Is crypto a security or a commodity? Should the SEC or CFTC take the lead?

Risks that new legislation is heavily influenced by the crypto industry itself.

“You’ve got a whole political party here that is always in the pockets of the big financial companies... so it’s always hard to legislatively do anything. That’s why we rely on regulators so often.”

-- Senator Sherrod Brown
What Makes This Hard?

you said a lot of stuff about how you wanted to make regulations, just good ones - was that pretty much just PR too?

Yesterday, 10:07 PM

there's no one really out there making sure good things happen and bad things don't

Yesterday, 10:07 PM

usually there's only one toggle--do more or do less

yeah just PR

fuck regulators

eyeah regulators

don't protect customers at all

Where Are We Headed?

Web3 is Going Just Great

...and is definitely not an enormous graft that's pouring lighter fluid on our already smoldering planet.

Created by Molly White (🐦, 🌐)

Lido token price tanks after podcaster spreads inaccurate rumor of Wells notice

It doesn't take much to tank a token price, particularly lately as fear of SEC action in the Ethereum staking world has run high. Popular podcaster David Hoffman speculated on his Bonkless podcast on March 3 that "I have wind that many, many, LDO price from March 2 to March 5, via CoinMarketCap $11.806 billion