CSCI 357: Algorithmic Game Theory

Lecture 20: Decentralized Currencies

Shikha Singh

Announcements and Logistics

- Project deadlines:
  - Check-ins this week (in progress): http://tinyurl.com/357sheet
  - In-class presentations on Friday: **10 mins with Q&A**
- Last AGT lecture today 
- End early today for SCS form

Questions?

End of Semester Get Together

When: Tomorrow!!

Time: starts at 11.30 am

(come after noon if you have class)

Project Report & Presentation

Project Report

- Final report (at least 6 pages, no more than 8 pages) due May 21st at 11 pm
  - Please organize content in a **coherent way** within the pages
  - Should look like a research paper in its structure and presentation
- For consistent in font & spacing, must use the LaTeX template provided: https://www.overleaf.com/read/tdqthvfvmrxt
- Submit Final report PDF and code (if applicable) via Github repository
  - Make sure to include a README file on how to run and test the simulation

Grading Rubric

- **Scholarship / Background:** Project involves reading, understanding, and contextualizing the most relevant research related to the topic. Write up adequately describes the background on the problem studied and how the approach is related to the existing literature. Resources used are appropriately cited.
- **Contributions:** Consistent with the timeline, and makes adequate contributions.
- **Correctness:** The work presented does not contain technical mistakes or logical gaps. Any programs written must be with clear documentation and a README on how they should be run to reproduce the results. Theoretical results should include correct and complete proofs.
- **Creativity:** Creative component: e.g., goes beyond what has been suggested by the instructor, this can include interesting empirical analysis, theoretical observations and insights, extensions or conjectures.
- **Presentation:** Approach and results are presented in a coherent and appealing way that makes it easy to follow. For example, **figures** and **examples** are used to explain concepts, and **data visualization or plotting** is used to convey empirical results.

Disclaimer: AI Tools

- **Okay to use for debugging/ searching for related papers/ figures/ visualization:**
    - Do not use it for text generation
- Cite the use AI tool when appropriate
    - Always distinguish your contribution from those that are borrowed
    - Can cite as a APA citation or just footnote/remark

Project Presentation Tips

- Your presentation will be graded
- **Sell the topic/work**. Pitch your work to the class
  - Why is it cool?
  - What were the interesting things you learnt/found?
  - Share your enthusiasm!
- **Challenges and techniques**. Share the challenges you faced and how you overcame them
- **Connect**. Tie to the topics we learnt in the class!

Presentation Tips

Tell a story

- What is the main takeaway message?
- Create a narrative around it
- Elements of a good story
    - *Characters, settings, the plot, the conflict, and the resolution*

Presentation Tips

Highlight your contributions & efforts

- **You** and **your work** is central to the theme
- Share **your** challenges
- How **you** overcame them (effort)
- What did **you** learn from this project?
    - Reflect on **your** work

Presentation Tips

Pictures and Commentary

- Use pictures: figures, graphs, clip arts!
- No one likes staring at a wall of text
- Point to draw attention!
- Text on slides is for the audience, not for you
    - Do not read slides word-for-word!

Presentation Tips

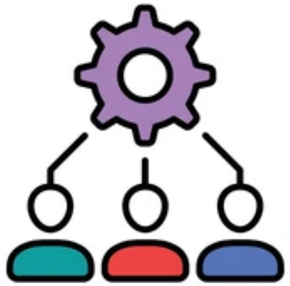
Less is More

- Don't try to cover too much!
- Be realistic about content that fits in 10 mins
    - Presentation vs report: each serve a different purpose
- A minute a slide is a good rule of thumb

Centralized Markets

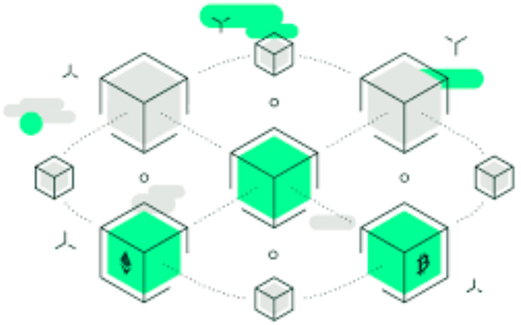
Centralized algorithm coordinates

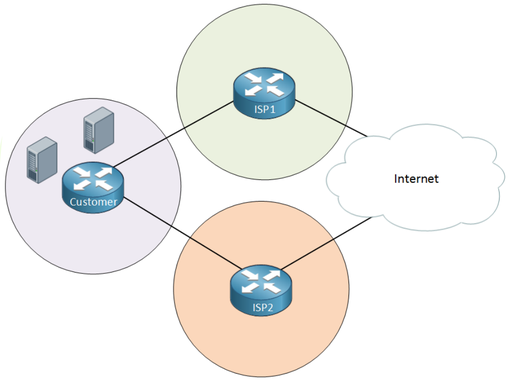
with Money



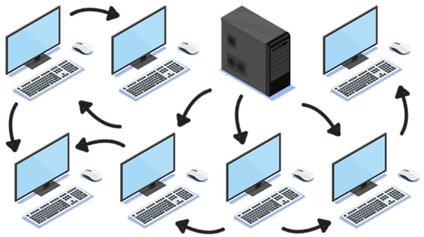
without Money

Decentralized Markets





No central authority: money is an option when trusted forms of exchange exist



BitTorrent Swarm

© TechTerms.com

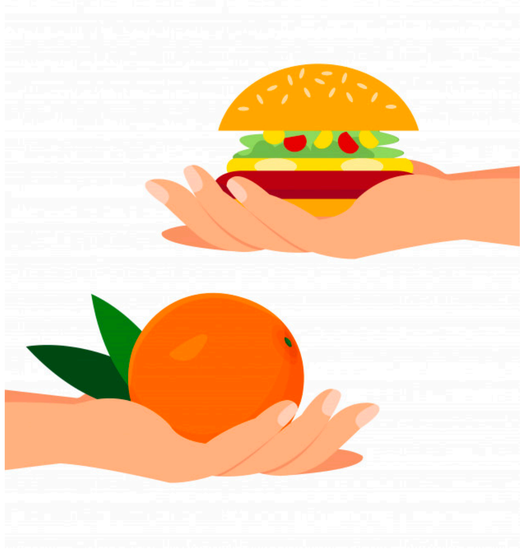
Decentralized "Money"

Let's talk about crypto

Crypto~~graphy~~ currencies

History of Money

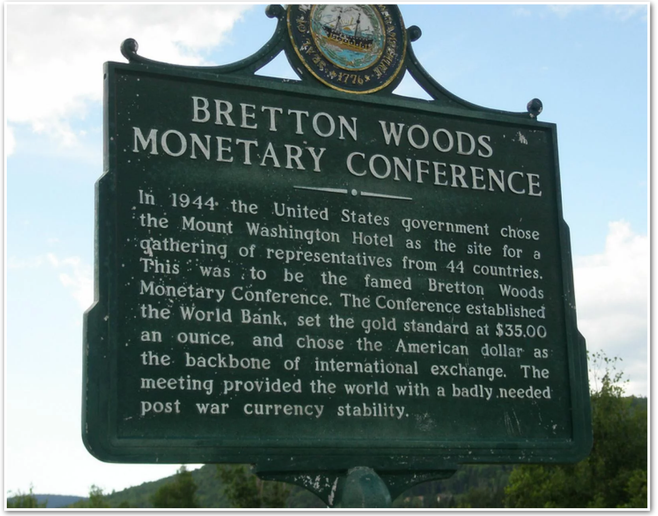
- Oldest form of exchange: barley
- Barter system followed: directly exchange goods or services
- Challenges with barter?
    - A **double coincidence of wants** at the same time
    - Physical proximity of trade
- Introducing money solves these problems
    - Money is transferable and divisible
    - Provides a standard form of value
- Money itself has gone through stages in history



Earliest Currency: Gold

Paper Money Backed by Gold

- When paper money was introduced: backed by **debt instruments**
    - Physical property that could be demanded in return
- **Gold standard:** governments would promise to exchange coins and paper notes at a fixed rate of gold
- In 1944, many nations joined the **Bretton Woods System**:
    - Agreed to tie its exchange rate to USD and US government guaranteed that USD could be converted to gold at a fixed rate



End of Gold Standard

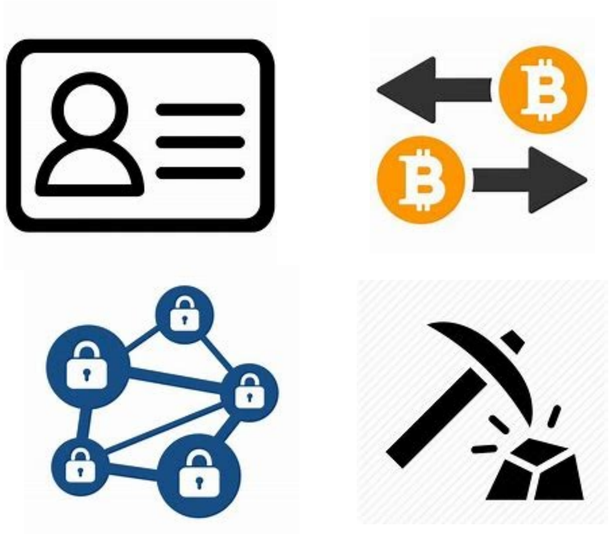
- In 1971 U.S. stopped conversion between USD and gold
- Collapse of gold standard:
    - Countries lost faith in the US dollar's value
    - Inflexibility of the system
    - Inability of a single country to have sufficient gold reserves

Fiat Money

- All major currencies today are fiat today
    - Fiat is Latin for "let it be done"
- Fiat money has no intrinsic value (no guarantee that it is worth something tangible)
- Value comes from a trust in the government or central bank that controls the money flow
    - Adding new money is inflationary (supply increases, value of each unit goes down)
- Governments have control over the currency and sustain its value by making it the standard medium of exchange

Decentralized Digital Money

- Does not rely on any centralized entity such as a government or central bank
- Allows money transfer by simply transferring bits
- Benefits claimed by proponents:
    - Lower cost (in theory)
    - Harder to regulate such P2P transactions
    - No reliance on central authority
- Downsides:
    - Hard to regulate means rife with fraud, illicit transactions, security attacks, forgery, etc
- Today's focus: incentives issues in P2P system such as blockchains



Credit: https://blockchain.berkeley.edu/

Centralized vs Decentralized Currency

Authenticity

Controlling money flow

Security against theft or fraud

Exchange value

Bitcoin

Bitcoin

- Created on Jan. 3, 2009 by a shadowy figure or a group working under the name Satoshi Nakamoto
    - Took hold post 2008 recession
- Anyone remember the first thing bought using Bitcoin?
- What's the value of BTC today?

Markets

10 Years After Laszlo Hanyecz Bought Pizza With 10K Bitcoin, He Has No Regrets

Laszo Hanyecz's 10,000 BTC pizza buy 10 years ago has a special place in bitcoin folklore, highlighting, however expensively, that participation is necessary for network success.

By Galen Moore · May 22, 2020 at 10:30 a.m. EDT · Updated Sep 14, 2021 at 4:44 a.m. EDT

Source: Coin desk

Source: https://yle.fi/uutiset/osasto/news/finance_ministry_crackdown_on_cryptocurrency_trade/10040789

Crypto giant FTX collapses into bankruptcy

Sam Bankman-Fried Sentenced to 25 Years in Prison

Mr. Bankman-Fried, who was convicted of stealing $8 billion from customers of his FTX cryptocurrency exchange, faced a maximum sentence of 110 years.

Share full article 1.4K

Just 18 months ago, Sam Bankman-Fried was a titan of the corporate world and was one of the youngest billionaires on the planet. Hiroko Masuike/The New York Times

Alex Mashinsky: founder of bankrupt crypto firm to plead guilty to fraud

CZ, founder of crypto giant Binance, pleads guilty to money laundering violations

The value of Bitcoin has topped $100k

Bitcoin to US Dollar, 31 Jul 2010 to 5 Dec 2024

Source: Bloomberg. Last update: 5 Dec 2024

BBC

Bitcoin

- Bitcoin is a fiat currency: a bitcoin has no intrinsic value
- Application built on top of the Bitcoin blockchain
    - Blockchain is what ensures the integrity of the currency
- So how does Bitcoin work?
    - The basic primitive is a transaction

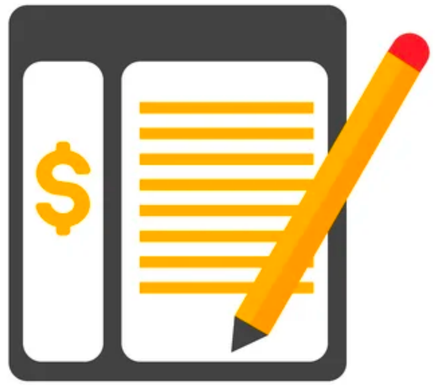
Source: https://yle.fi/uutiset/osasto/news/finance_ministry_crackdown_on_cryptocurrency_trade/10040789

A Bitcoin Transaction

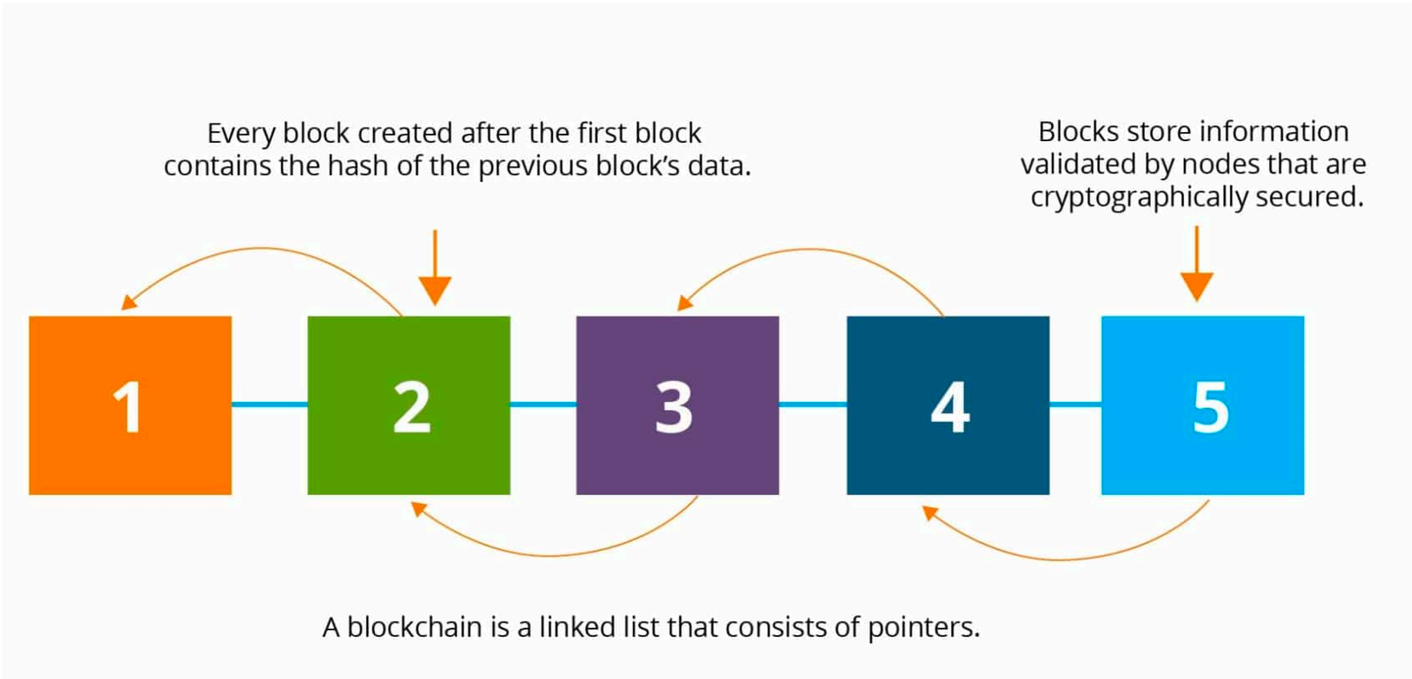
- Much like a credit-card transaction except it requires
  - Senders and receivers identified by their public keys
  - Proof of ownership of the coins being transferred in the form **of a pointer back to most recent transactions** involving the transferred coins
- A transaction is **valid** if:
  - it has been cryptographically signed by all the senders (verified using the sender's public key)
  - the sender is a valid owner of the coins being sent

Source: https://yle.fi/uutiset/osasto/news/finance_ministry_crackdown_on_cryptocurrency_trade/10040789

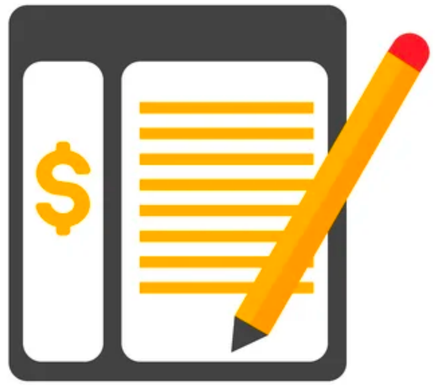
Bitcoin Blockchain



- All transactions are written to a decentralized ledger (Bitcoin blockchain)
  - A giant P2P shared write only google sheet essentially
  - Linked-list structure



Minting New Coins



- In a centralized system, central bank mints new currency
- In decentralized, anyone can create new a bitcoin block
  - **Incentive to mine**: **Block reward** of a new block (flat rate) to miner: exponentially decays over time
  - Initially was 50 BTC, but the protocol dictates that this amount gets halved every four years (Is now 3.125 BTC)
- On finding a valid block, a miner broadcasts the block the network
- A new block of transactions involves a **proof of work**: the authorizer has to solve a computationally difficult puzzle

Proof of Work

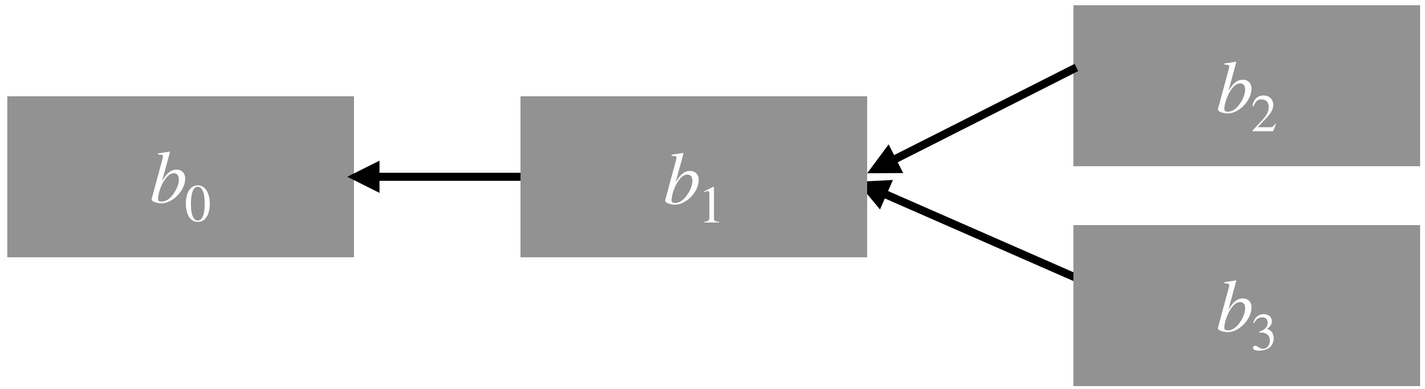
- Proof that certain amount of "computational effort" has been expended
- Very computationally intensive
  - Recent estimates from the University of Cambridge put Bitcoin's energy consumption **as equal to that of Switzerland**
- Difficultly level of the puzzle is chosen to keep the rate of valid block creation roughly constant: averaging around 1 block every ten minutes
  - Why 10 minutes? To keep block creation rate slower than the latency in peer to peer network!

Consensus

- Each node in the P2P system has a its own local "view" of the blockchain
- Consensus is reached on what the central ledge consists off through various distributed consensus protocol
    - Many forms, essentially rely on a majority voting rule

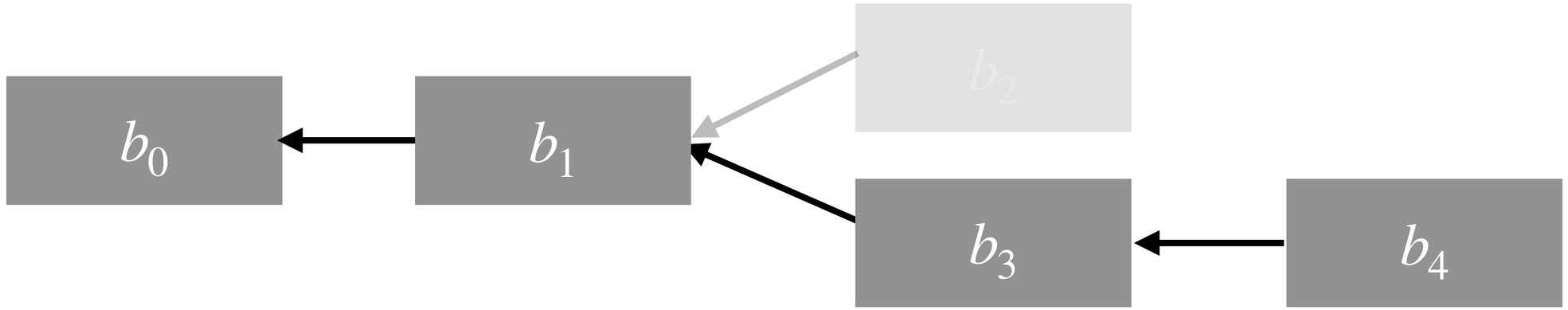
Forks

- If two different miners discover valid blocks roughly at the same time, it results in a fork in the blockchain
- The mechanism by which everyone decides the "right" branch
    - A user should regard the longest branch as the valid one
- At this point, different users have different opinions on which branch is right based on when they heard about it



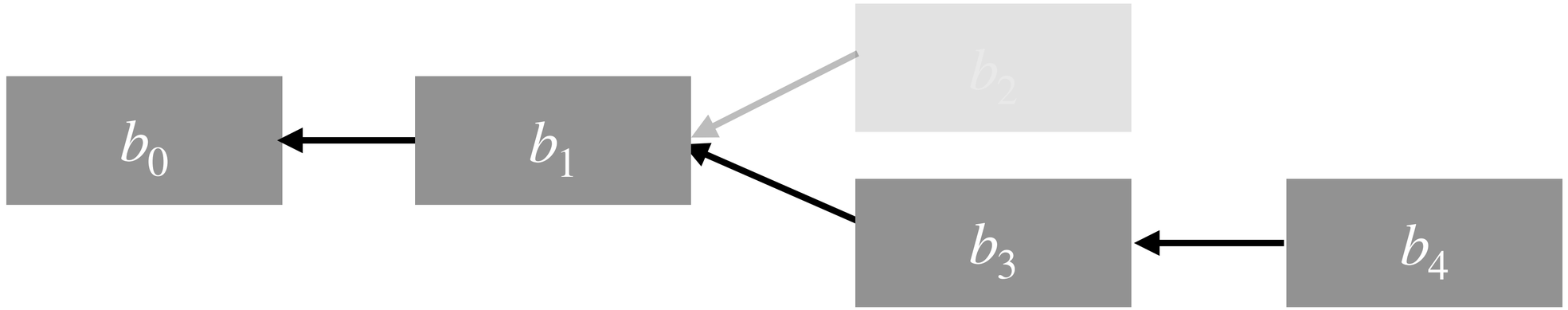
Forks

- Eventually, some miner is going to extend on the branches
- When this happens, users have a consistent view
    - the longer branch is adopted as the blockchain
    - the shorter branch is "orphaned"



Authorized Transaction

- A seller does not regard a transaction as authorized until it is included in the blockchain and also has been extended
    - Conservative sellers may wait for some $k \geq 1$ number of blocks to follow
- Transaction fee must be paid by seller: not low, around 20$ right now



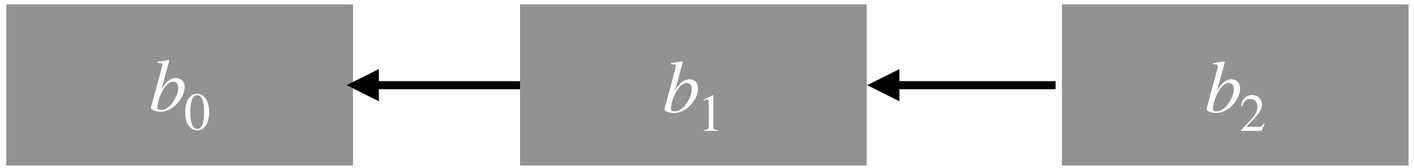
Incentives & Attacks

Sybil Attack

- Bitcoin users are identified by their public key
- It is easy and inexpensive to create many public keys, so many Bitcoin users may correspond to the same person
- Deliberately creating multiple identities in a system is a called a Sybil attack
- Sybil attacks do not cause much issue in Bitcoin
    - Influence is determined directly by computational power
    - "One CPU one vote"

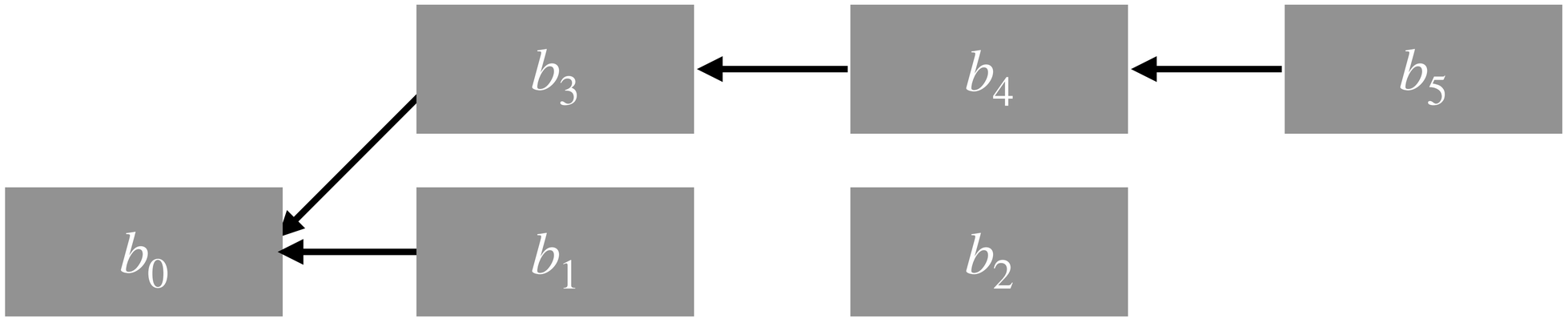
Double-Spend Attack

- Miners may deliberately create forks in the blockchain to "double spend"
- Suppose in transaction T, Aamir transfers some bitcoins to Beth, and T is added to the blockchain as part of block b_1
    - Beth waits for b_2 to the added and then ships the goods to Aamir



Double-Spend Attack

- When Aamir gets the goods, he can:
  - Try to find a valid block b_3, b_4 and b_5 extending b_0 in a longer chain
  - If Aamir creates these before another miner extends b_2, then he has successfully "ripped off" Beth



Mining Power

- How likely is Aamir to succeed in such attacks?
    - Depends on how much computational power he has
- Suppose Aamir controls an α fraction of all computational power being devoted to Bitcoin mining (mining power)
    - α essentially is Aamir's chance of finding a valid block by brute force
    - Finding three valid blocks happens with prob α^3

Mining Pools

- Success of double-spend depends on the mining power of a user
- For a solo miner, α is not very big
- But what can cause problems?
    - Many miners, however, participate in **mining pools**
    - Act as a collusive team and split rewards
- Big mining pools can control a significant fraction of the computational power
    - For example, $\alpha = 0.3$

51% Attack

- When mining pools can consolidate to control more than half of mining power:
    - On average creates more than every other block
    - Can keep extending the chain and eventually overtake any other chain
- Bitcoin is not intended to function under concentration of power
    - Such an entity effectively acts as a centralized authority!

Concentration of Power

- In 2019, "over 70% of the transactions on the Bitcoin network were going through just four Chinese companies"
- Bitcoin mining uses specialized hardware: first GPUs, and now ASICs (application specific integrated circuits) which promotes concentration of power

Bitcoin's 'One Percent' Controls Lion's Share of the Cryptocurrency's Wealth

New research shows that just 0.01% of bitcoin holders controls 27% of the currency in circulation

BBC

China declares all crypto-currency transactions illegal

24 September 2021

Share Save

China's central bank has announced that all transactions of crypto-currencies are illegal, effectively banning digital tokens such as Bitcoin.

Selfish Mining

- Another type of deviation: **block withholding**
- Suppose Aamir found a valid block b
- What is the incentive for Aamir to withhold broadcasting b?
  - Intuition: Aamir can trick other miners into working on the wrong puzzle (extending the last publicly announced block)
  - Meanwhile, Aamir can privately try to extend his own block
    - Has an advantage: not competing with others
- This is called the selfish mining strategy
- How good of a strategy is this? Is it be profitable?

Selfish Mining

- **(Eyal and Sirer).** If a user's mining power α is bigger than $1/3$, and all other miners are honest, then selfish mining yields greater expected reward than honest mining
    - Original white paper by Nakamoto, suggested than Bitcoin suffered from no incentive issues as long as no miner controlled more than $50\,\%$ of the power
    - Eyal and Sirer show that honest mining is not an equilibrium

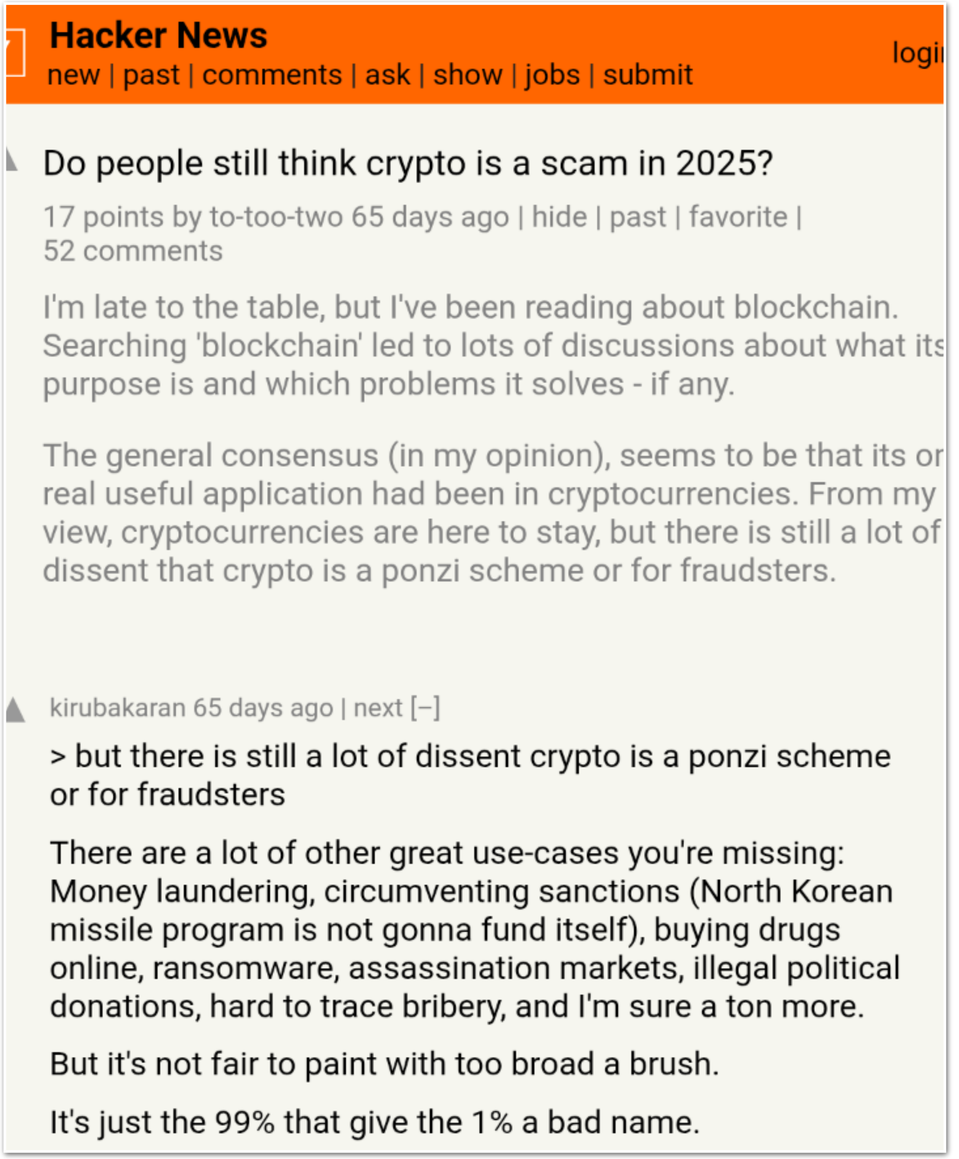

DOI:10.1145/3212998

Majority Is Not Enough:
Bitcoin Mining Is Vulnerable

By Ittay Eyal and Emin Gün Sirer

Takeaways

- No consensus on where things are going
  - Mostly has been used to avoid regulation even a decade and a half into it
  - Creating more problems than it is solving?
- Case study in the trade offs between **centralized** and **decentralized** market
- Perhaps a good ad for why to take this course?
  - Why computer scientists need to understand ethics, policy and market design



Academic Involvement

- Contributions to specific components and tech
  - Consensus
  - Distributed hash tables
  - Cryptographic protocols
  - Study of incentives and equilibrium

Transaction Fee Mechanism Design for Leaderless Blockchain Protocols

Pranav Garimidi[1], Lioba Heimbach[2*], and Tim Roughgarden[1,3**]

[1] a16z crypto pgarimidi@a16z.com
[2] ETH Zurich hlioba@ethz.ch
[3] Columbia University tim.roughgarden@gmail.com

Collusion-Resilience in Transaction Fee Mechanism Design

HAO CHUNG, Carnegie Mellon University, USA
TIM ROUGHGARDEN, Columbia University and a16z crypto, USA
ELAINE SHI, Carnegie Mellon University, USA

timroughgarden.org/s25/

COMS 4995-001: The Science of Blockchains, Spring 2025

Announcements

- Jan 22: Welcome to COMS 4995-001!

Instructor: l

- Tim Roughgarden (Office hours: Mondays/Wednesday after class (until 10:45am), in Mudd 410. Email: tim.roughgarden@gmail.com.)

Algorand

Meet The Women Of The Blockchain: Elaine Shi, Chief Scientist at ThunderCore

Tim Roughgarden became head of Research for a16z crypto

SCIENCEINSIDER | SCIENCE AND POLICY

Exclusive: NSF faces radical shake-up as officials abolish its 37 divisions

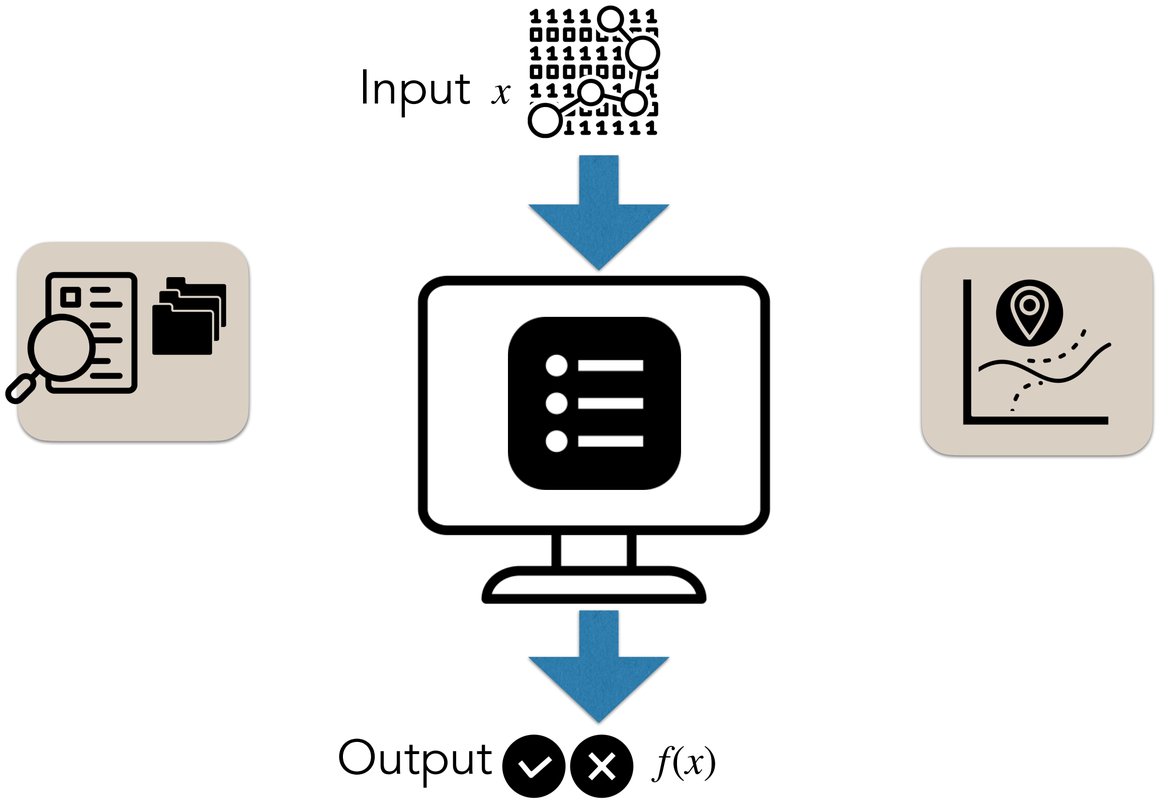
Changes seen as a response to presidential directives on what research to fund

8 MAY 2025 · 6:25 PM ET · BY JEFFREY MERVIS

Course Wrap Up

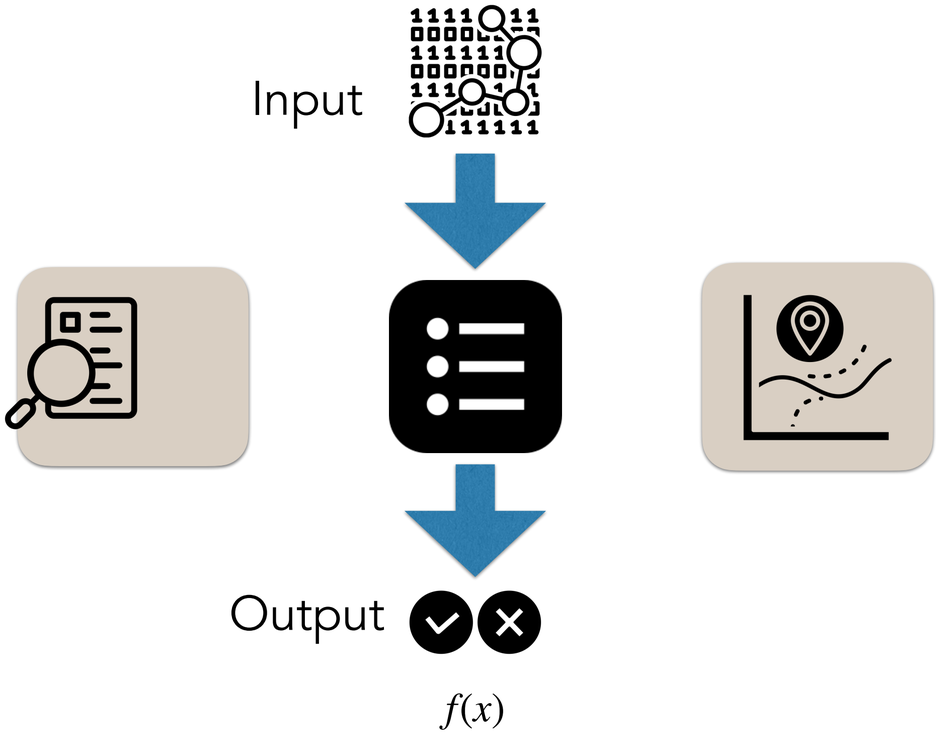
What is Algorithmic Game Theory?

Algorithms



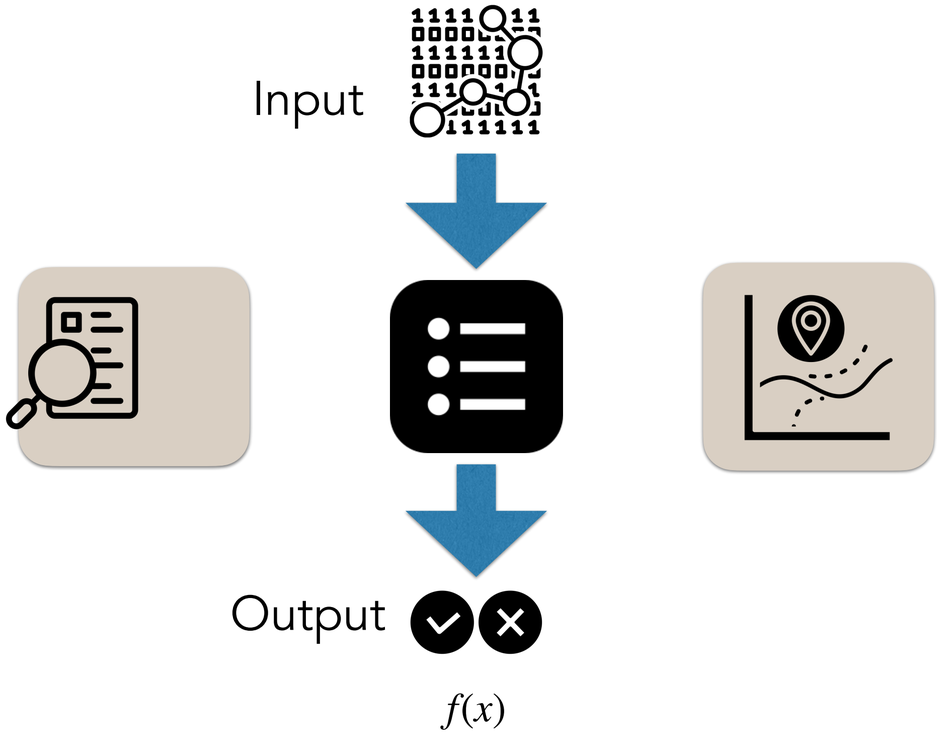
Classic View of Algorithms

- Focus on **running time**
- Availability and integrity of input is taken from granted

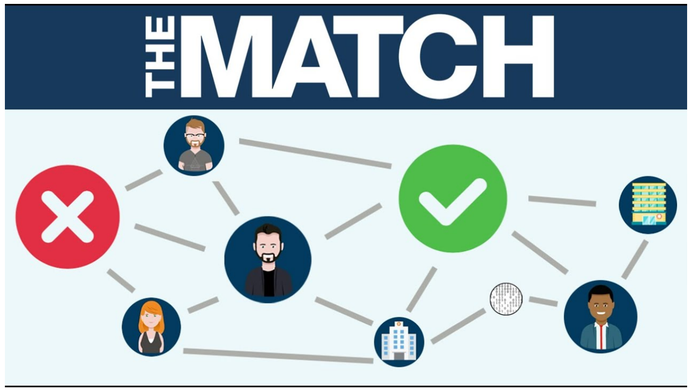


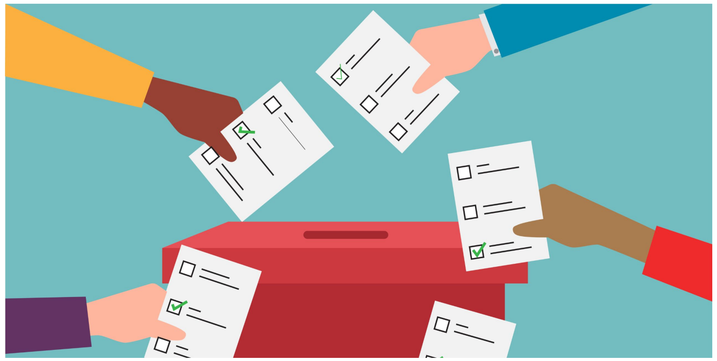
"Real World" Algorithms

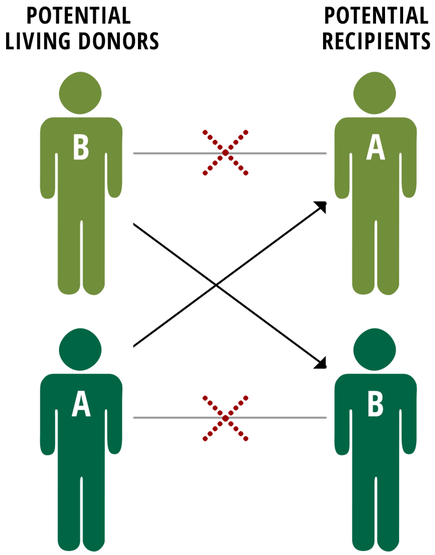
- Input is based on people's private information (preferences or beliefs)
- Output is an allocation or decision or outcome that has a social cost

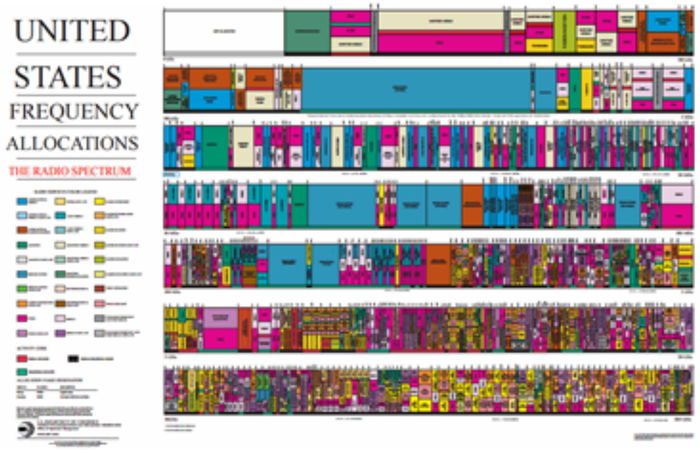


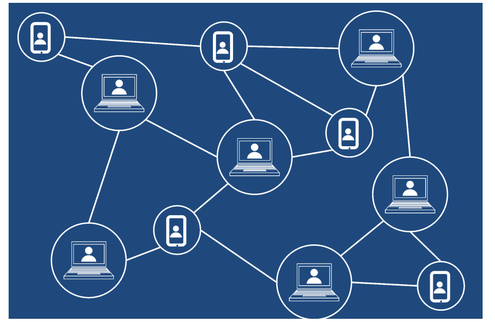
"Real World" Algorithms





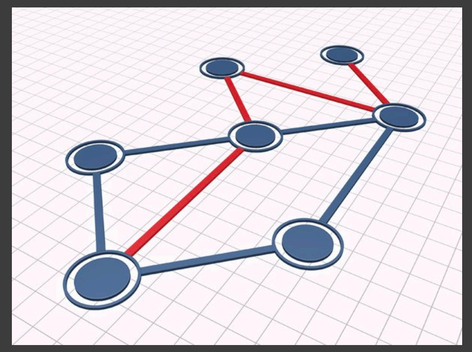




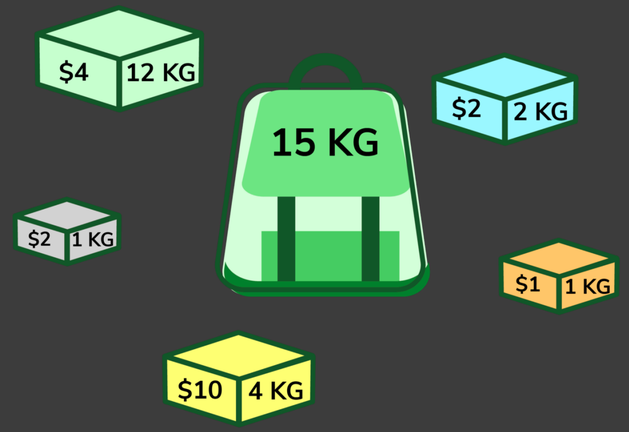


How does strategic behavior affect the outcome of an algorithm? And how it can and should influence system design?

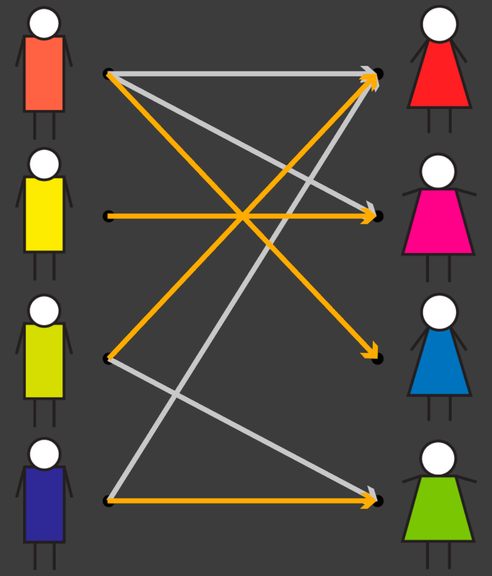
How to align system designer's objective with that of participants?



Routing in Networks



Resource allocation



Matching problems

Algorithmic Game Theory: Topics

Game Theory Basics

Mechanism Design with Money

Auction Theory

Application: **Sponsored Search**

Mechanism Design without Money

Matching Markets Theory

Social Choice Theory

Applications: School Choice, Voting Rules

Decentralized Games in CS **Applications**

Incentives in BitTorrent

Incentives in Network Routing

Incentives in Cryptocurrencies

Cocktail Napkin Stories

Prisoner's Dilemma

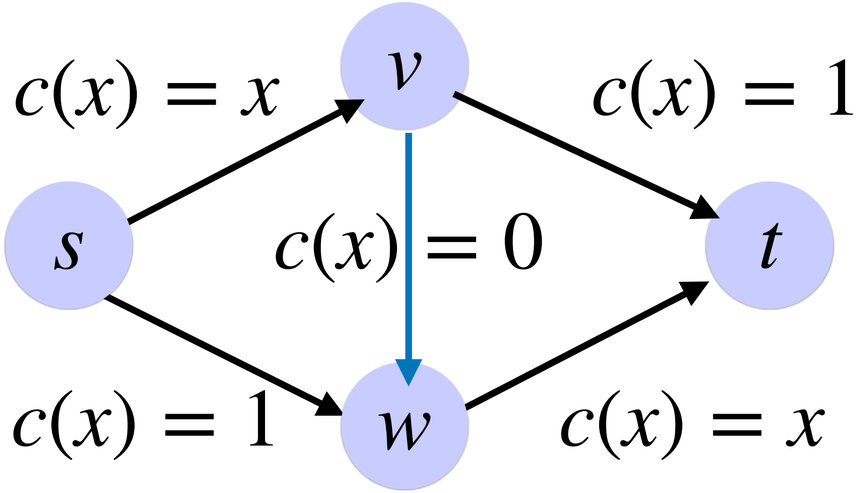
Revenue Equivalence

2/3rds Game

Envy-free Cake-cutting!

$$n^{n^{n^{n^{n}}}}$$

Braess Paradox



Secondary Goals:

- Algorithmic impact on other fields (policy, politics, economics)
- Running time is not the only performance metric for an algorithm
    - Strategyproofness / Incentive compatibility
    - Fairness and social welfare
- What does research in this topic look like?
    - Reading and analyzing research papers
    - Demystify the research process through projects

AGT Mindset: Rules Matter!

- Many badly designed systems around us that do no take incentives and strategic behavior into account
- Strategic behavior may seem counter-intuitive, but AGT teaches you
  - How to reason about it systematically and formally
  - How to leverage this behavior to the benefit of the system
- Favorite part about this course: grounded in real-life applications
  - Theory might make assumptions, but on the whole has proven very useful in practice

Biggest Takeaways:

Learning to think game-theoretically which informs good practices in algorithm design

Thank you!

- You all should be proud of how much you've learned
  - Grad level course!
- **Thank you** for your engagement and enthusiasm during the semester
- Good luck on the project presentations & report and have great well-deserved summer break!

Course Evaluations

OPTIONAL SCRIPT FOR PROMOTING THE STUDENT COURSE SURVEY

Every term, Williams asks students to participate in end-of-semester course evaluations. Your feedback will help improve this course for other students taking it in the future, and help shape the [department/program name] curriculum.

You may skip questions that you don't wish to answer, and there is no penalty for choosing not to participate. All of your answers are confidential and I will only receive a report on your responses after I have submitted all grades for this course. While evaluations are open, I will receive information on how many students have filled out the evaluations, but I won't be told which of you have and haven't completed them. I won't know which responses are associated with which student unless you identify yourself in the comments.

To access the online evaluations, log into Glow (glow.williams.edu) using your regular Williams username and password (the same ones you use for your Williams email account). On your Glow dashboard you'll see a course called "Course Evaluations." Click on this and then follow the instructions on the screen. If you have trouble finding the evaluation, you can ask a classmate or reach out to Institutional Research at ir@williams.edu. The evaluations are open to you from now through the end of reading period. If you haven't filled it out by the beginning of reading period, you will start receiving email reminders.

Course Evals TL;DR

- Two parts: **(1) SCS form** , **(2) Blue sheets** (both on GLOW)
- Your responses are **confidential** and we will only receive a report of your anonymized comments after we have submitted all grades for this course
- **SCS forms** are used for promotion and seen by college committee, **blue sheets are open-ended** comments directed only to your instructor

*To access the online evaluations, log into **Glow** (glow.williams.edu) using your regular Williams username and password (the same ones you use for your Williams email account). On your Glow dashboard you'll see a course called "**Course Evaluations**." Click on this and then follow the instructions you see on the screen. If you have trouble finding the evaluation, you can ask a neighbor for help or reach out to ir@williams.edu.*