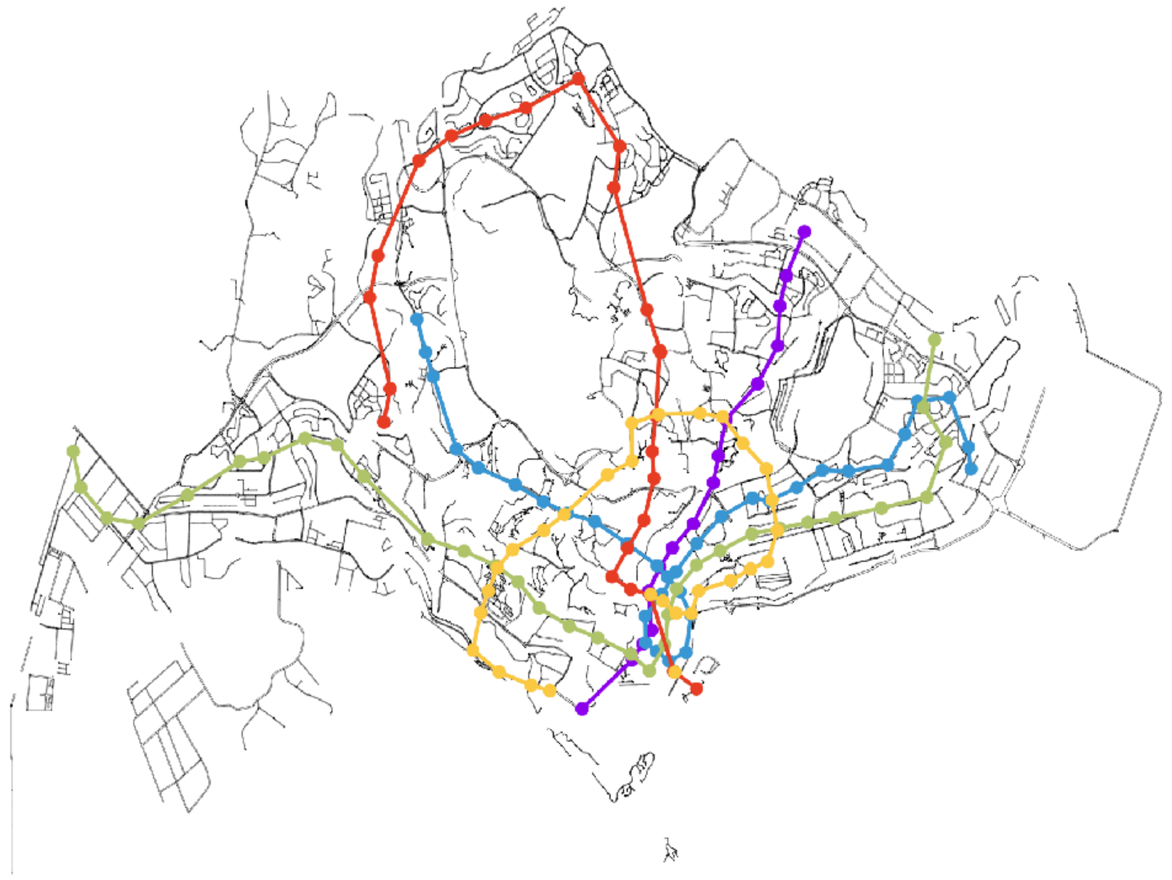
CSCI 357: Algorithmic Game Theory

Lecture 22: Incentives in Bitcoin & Wrap Up

Shikha Singh



Announcements and Logistics

- 2-page report (which includes background) due Friday 5 pm
- Final report due May 19 (Thursday) 11 pm
- Next week: student presentations in class
  - Schedule has been posted
  - 6 presentations on Monday, 8 on Thursday based on preferences
  - Presentations must be no more than 8 mins
  - Each talk will be followed by 1.5 mins for questions
  - Must send **your slides to me by 2 pm** on the day of presentation
- Project meetings: sign up at https://tinyurl.com/357projectmeet

Questions?

Class of 60s Talks

Suresh Venkatasubramanian

Thursday, May 05 @ 7:30pm
Bronfman Auditorium – Wachenheim

Machine Readable: The Power and Limits of Algorithms that are Shaping Society

Friday, May 06 @ 2:35 pm
Wege, TCL 123

On Equity in Access

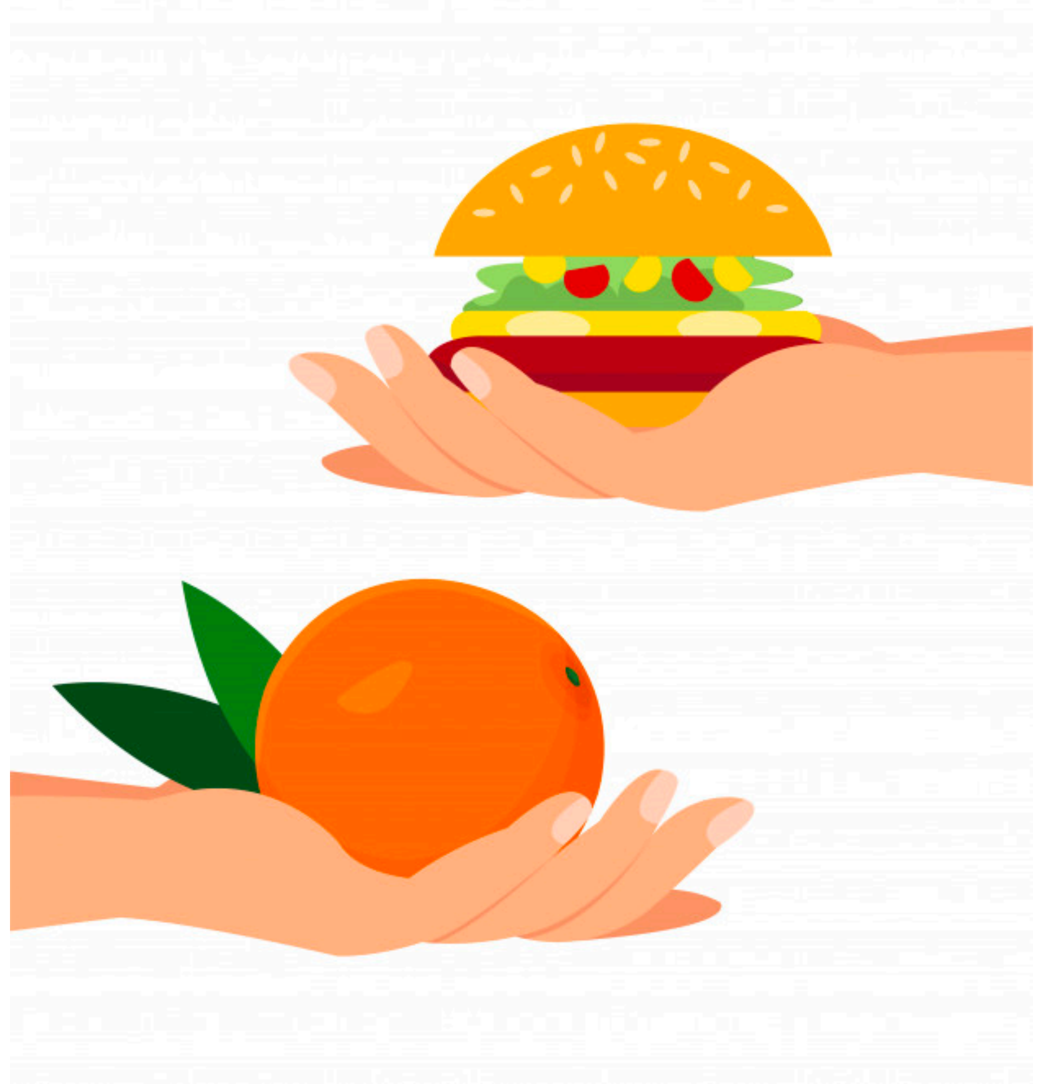
Plan

- Wrap up the ongoing unit on incentives in P2P networks
  - Started with BitTorrent (file sharing)
  - Selfish routing in local area networks
  - Incentives in BGP routing
- Today: Short lecture on incentives in cryptocurrencies (Bitcoin)
- Course overview wrap up + **SCS forms**

Role of Money

History of Trade & Currency

- 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



The Gold Standard

- Until the 16th centuries, money took the form of metal coins
- When paper money was first introduced, it was backed by debt instruments
    - The physical property that could be demanded if return for some paper money
- **Gold standard**: governments would promise to exchange coins and paper notes at a fixed rate of gold
- In 1944, many leading nations joined the **Bretton Woods System:** each country agreed to tie its exchange rate to US dollar and US government guaranteed that US dollars could be converted to gold at a fixed exchange rate

End of Gold Standard

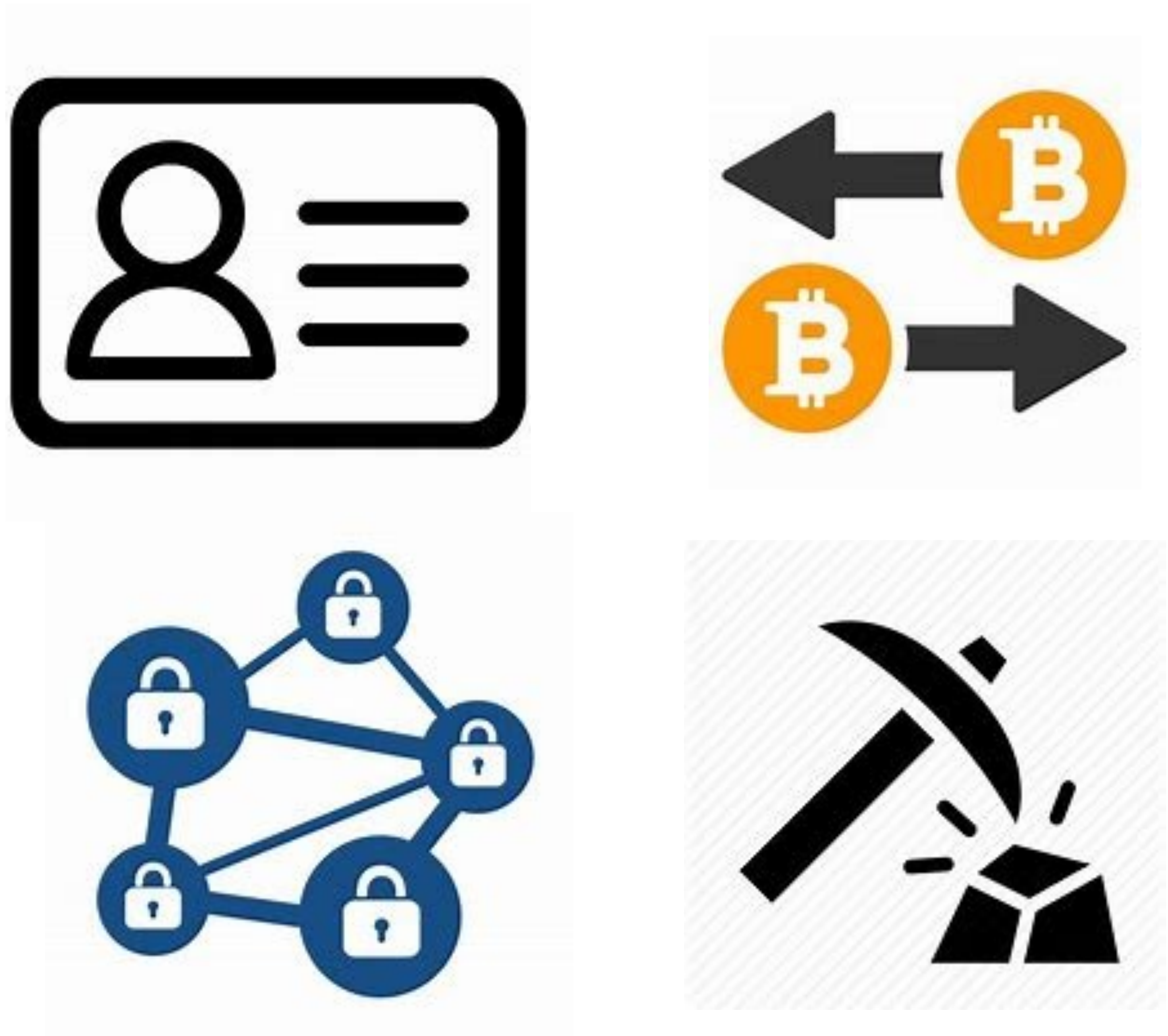
- On August 15, 1971 U.S. stopped conversion between U.S. Dollars and gold
- Collapse of gold standard:
    - US currency became too overvalued
    - Other countries started exchanging money for gold or leaving the system
- Challenges of this system:
    - Inflexibility (governments often control cash flow, by increasing monetary supply)
    - Hard to sustain with limited 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

Digital Money

- Does not rely on any centralized entity such as a government or central bank
- Allows money transfer by simply transferring bits
- Benefits?
  - Lower cost (in theory): avoids transaction fees
  - Harder to regulate such P2P transactions
  - No reliance on central authority
- Downsides?
  - Bugs, security problems, unintended behavior
  - Incentive attacks



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

Digital Currency vs Regular

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
- Most successful digital currency
- As of Wednesday Dec 2, **1 BTC = 37,038.90USD**
  - This has fluctuated over time
- Anyone remember the first thing bought using Bitcoin?

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

Bitcoin BTC

USD

XBX

Buy / Sell

$37,114

24H %	-4.22%
24H Low	$36,639.73
24H High	$40,002.75

CoinDesk

Bitcoin

- Bitcoin is a fiat currency: a bitcoin has no intrinsic value
- Bitcoin is an application that is 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

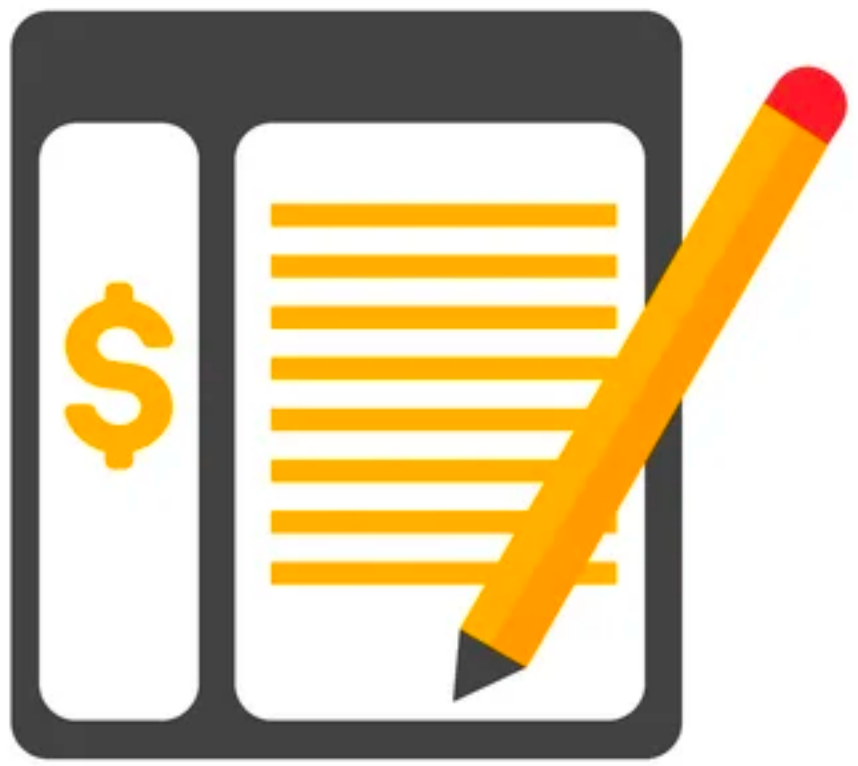
- A transaction has the following components:
  - One or more senders
  - One or more receivers
  - The amount of BTC (Bitcoins) transferred from each sender to each receiver
  - A proof of ownership of the coins being transferred in the form of a **pointer** back to most recent transactions involving the transferred coins
  - A **transaction fee**, paid by the sender to the authorizer of the transaction

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

A Bitcoin Transaction

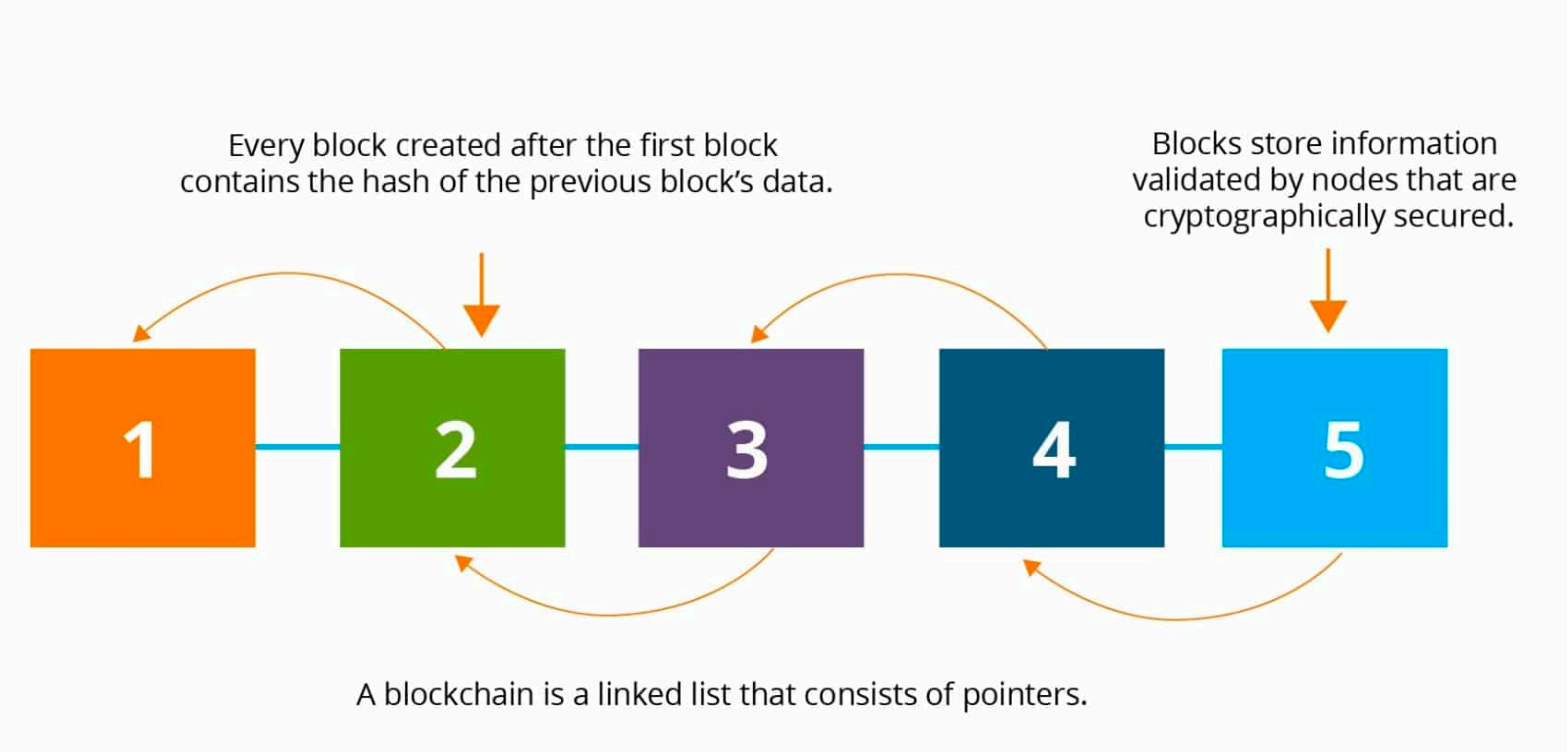
- Senders and receivers are identified by their **public keys**
- A transaction is **valid** if:
    - it has been **cryptographically signed** by all the senders (verified using the sender's public key)
    - the sender is a **valid owner of the coins being sent**
- How do we verify who owns which coins?
    - All transactions are **broadcast to all other users** (over a P2P network) and all users keep track of all transactions that have ever been authorized

Bitcoins Blockchain



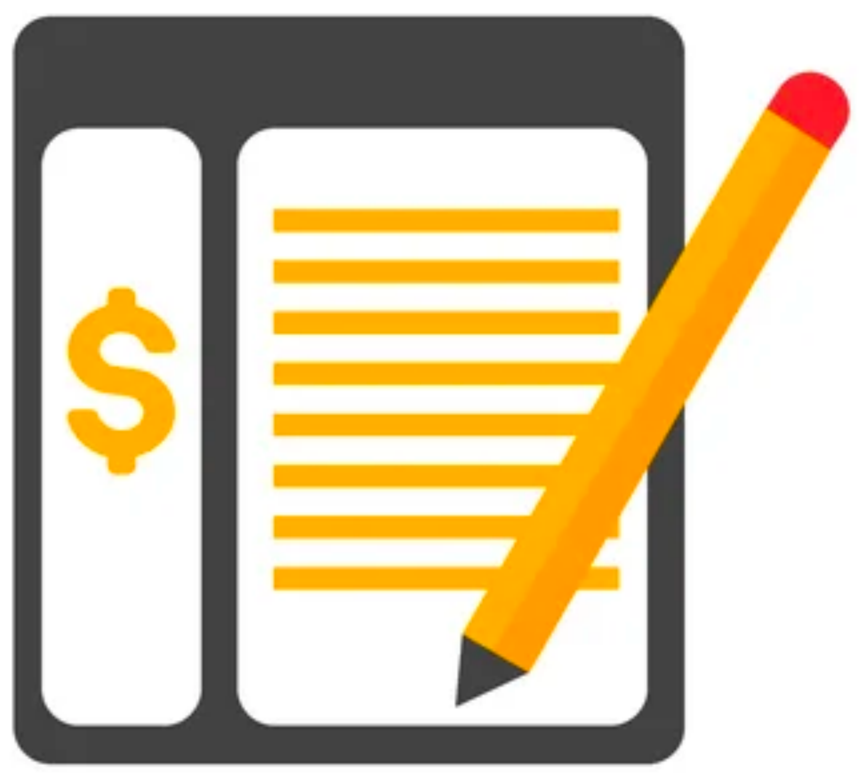
- The record of all transactions: **the ledger**
- **Blocks**: a group of transactions (~1000-2000, 1 MB cap on block size)
- Contains the following:
  - One or more **transactions**
  - A **hash of the previous block**
  - A **nonce**
- We end up with a linked-list type structure called the **blockchain**

Blockchain Structure



https://intellipaat.com/mediaFiles/2019/02/blockchain-as-linked-list-1.jpg

Adding Blocks



- How do transactions get created and added to the ledger?
    - Anyone can create a block, but why would they do it?
    - The first transaction in the block is a flat-rate payment of Bitcoins to the miner (**block reward**)
    - These are brand new Bitcoins, which increases the number of bitcoins in circulation
- On finding a valid block, a miner broadcasts the block the network
- To avoid anarchy and congestion, a new block of transactions involves a **proof of work**: the authorizer has to solve a computationally difficult puzzle

Proof of Work

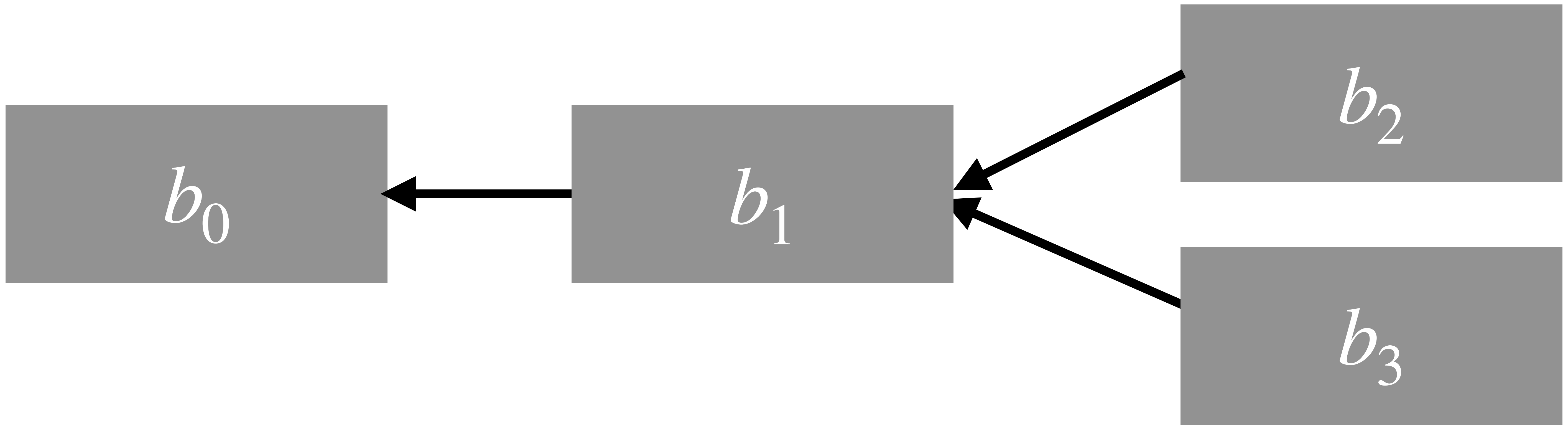
- Form of cryptographic proof in which the miner proves to others that a certain amount of a computational effort has been expended
- Generally done by inverting a one-way cryptographic hash function, e.g. SHA-256
    - Best approach (brute force)
    - Very computationally intensive
    - Recent estimates 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!

Reward and Fee

- Block reward:
  - Initially this was 50 BTC, but the protocol dictates that this amount gets halved every four years
  - Is now 6.25 BTC
  - Decays exponentially with time (can only ever have 21 million BTC, unless the protocol is changed)
- The second amount is the sum of the **transaction fees** in the block (paid by sellers whose transaction is in the block: like credit card transaction fee)

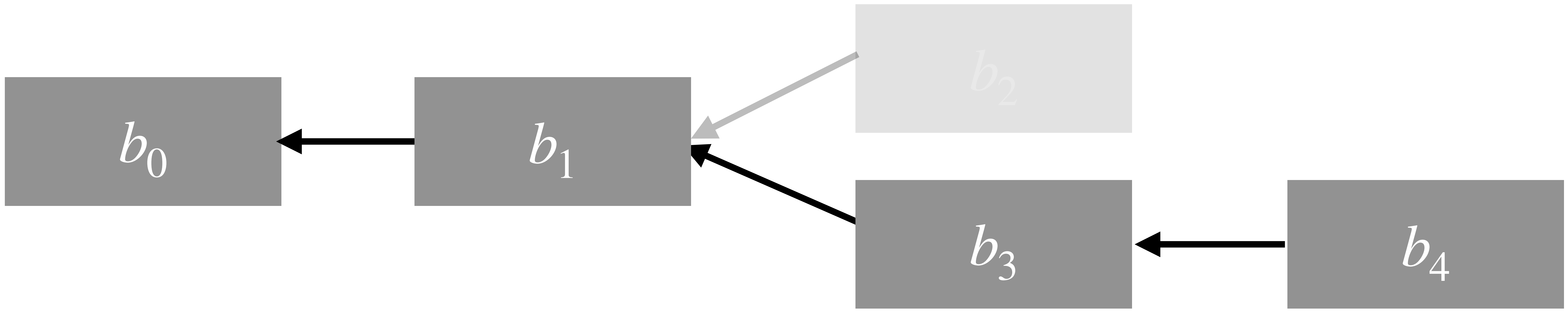
Forks

- 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



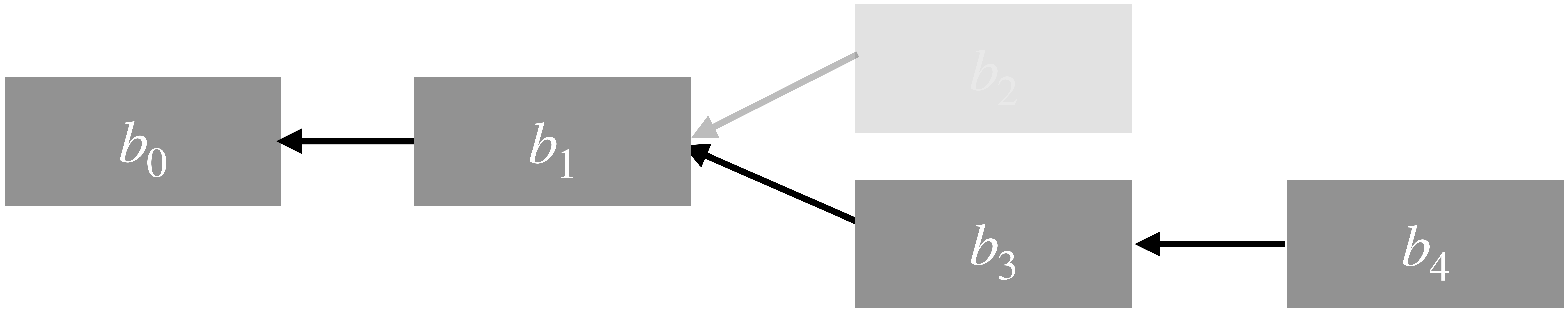
Forks

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



Authorized Transaction

- Blocks occasionally get orphaned even when all miners are following the protocol
- A seller does not regard a transaction as authorized until it is included in the blockchain **and also** has been extended
    - More conservative sellers may wait for some $k \geq 1$ number of blocks to follow



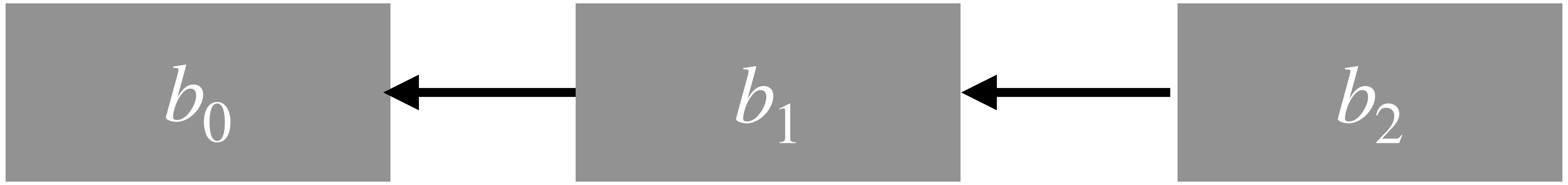
Incentives & Attacks

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"**

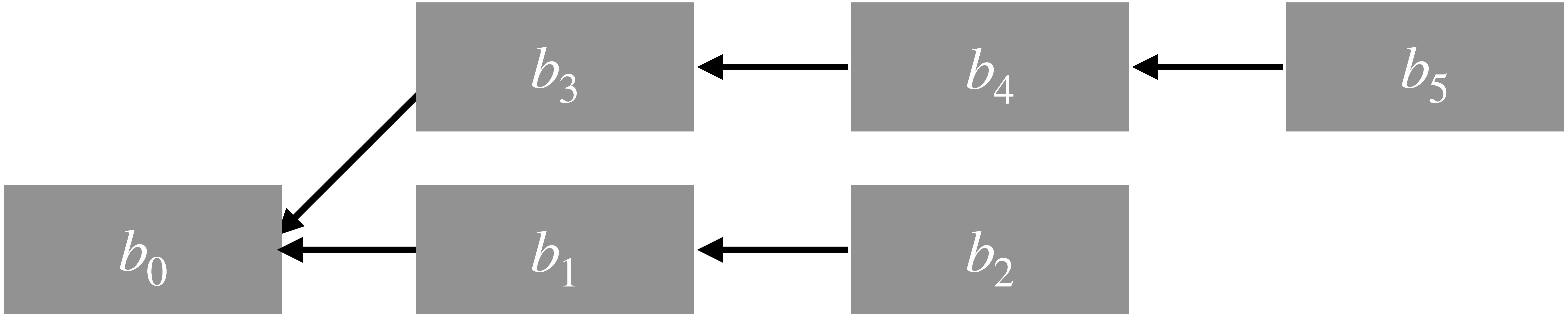
Double-Spend Attack

- Miners may deliberately **create forks in the blockchain**
- Creating forks can let users "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 could try the following attack:
  - Try to find a valid block b_3, extending b_0, another block b_4 extending b_3 and a third block b_5 extending b_4
- 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?
- The probability that Aamir succeeds in his double-spend attack depends on how much computional power he has
- Suppose Aamir controls an α fraction of all computational power being devoted to Bitcoin mining
  - Called Aamir's mining power
- α essentially approximates Aamir's chance of finding a valid block by brute force
  - Finding three valid blocks happens with prob α^3
- More generally if Beth waits for k blocks to be appended to the b_1, then the probability of a successful attack is α^{k+2}

Mining Power

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

51% Attack

- The probability of success of double spend is roughly $1/8$, even when alpha is slightly above $1/2$
- But when $\alpha > 1/2$, a more patient strategy works
  - Since Aamir controls more than half of the mining power, on average Aamir creates more than every other block
  - If Aamir continues to extend her own chain $(b_3, b_4, b_5, \ldots)$ eventually it will overtake any other chain
- In general, Bitcoin is not intended to function when a single entity controls more than half of the power
  - Such an entity effectively acts as a centralized authority!

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 is that Aamir can trick other miners into working on the wrong computational problem (extending the last publically announced block)
  - Meanwhile, Aamir can privately try to extend his own block
- This is called the selfish mining strategy

Selfish Mining

- Suppose the last block announced was b_0
- Aamir discovers a new valid block a_1 extending b_0 which he keeps secret
- The selfish mining strategy says:
    - Work privately to extend your private chain, unless some other miner finds and extends b_0 by a chain longer by 1
- That is, Aamir always tries to maintain a lead of one, if Aamir fails he must give up and lose the reward of the withheld block
- 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
- The 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
- So what are the equilibria?

DOI:10.1145/3212998

Majority Is Not Enough: Bitcoin Mining Is Vulnerable

By Ittay Eyal and Emin Gün Sirer

Concentration of Power

- *"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
- Has motivated other kinds of "proof-of-work" protocols

How China Took Center Stage in Bitcoin's Civil War

Gilles Sabrie for The New York Times

By Nathaniel Popper

Just the Beginning

- Very few courses on the topic but growing
- Big push in AGT and TCS to establish the theoretical foundations
- Many avenues for AGT and CS:
  - Building consensus (voting)
  - Charging the correct transaction fee (mechanism design with money)
  - Computationally difficult problems
  - Security, privacy, and ethics

Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559*

Tim Roughgarden†

December 3, 2020

Dynamic Posted-Price Mechanisms for the Blockchain Transaction-Fee Market

Matheus V. X. Ferreira
mvxf@cs.princeton.edu
Princeton University
Princeton, New Jersey, USA

Daniel J. Moroz
dmoroz@g.harvard.edu
Harvard University
Cambridge, Massachusetts, USA

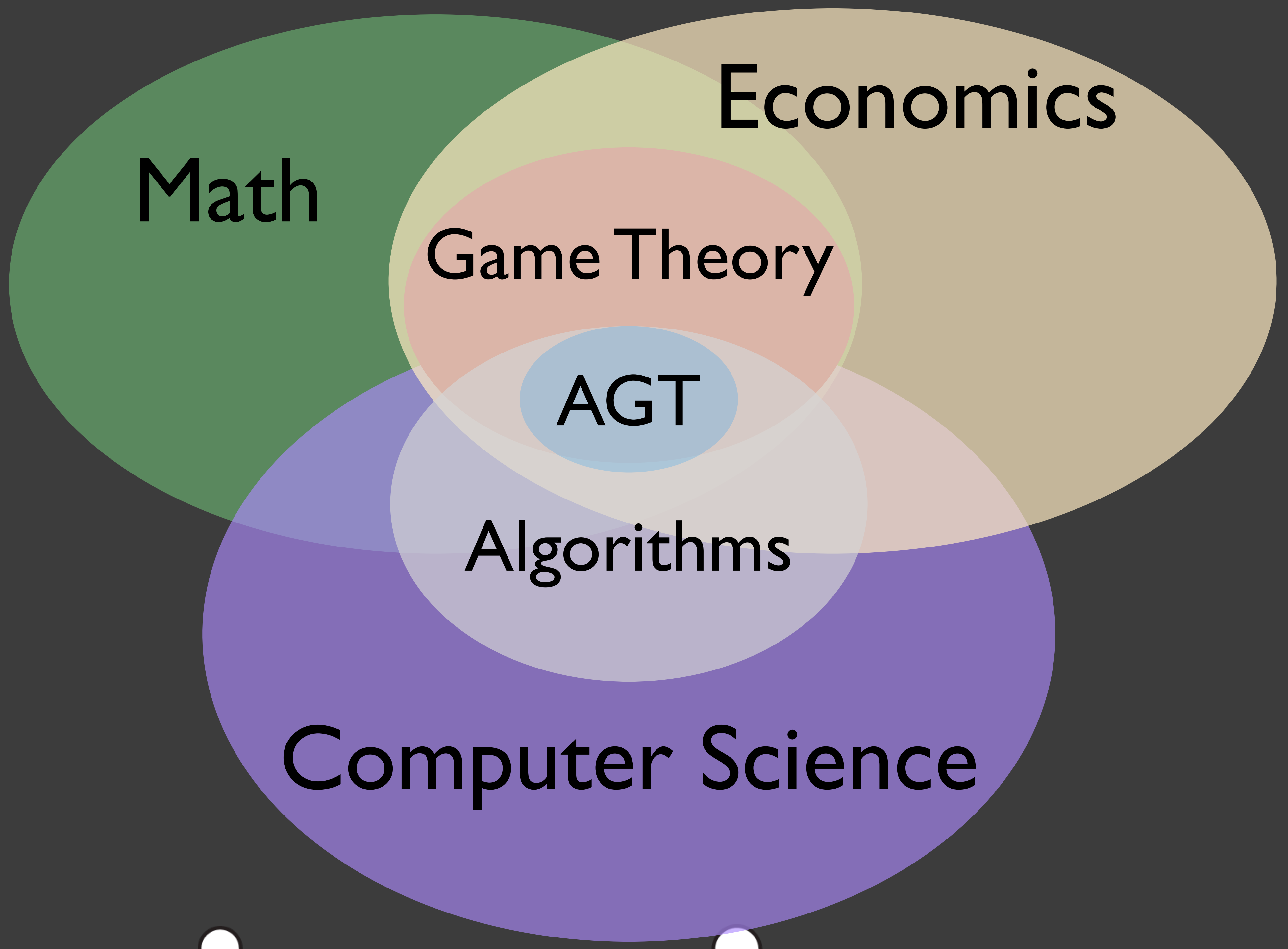
David C. Parkes
parkes@eecs.harvard.edu
Harvard University
Cambridge, Massachusetts, USA

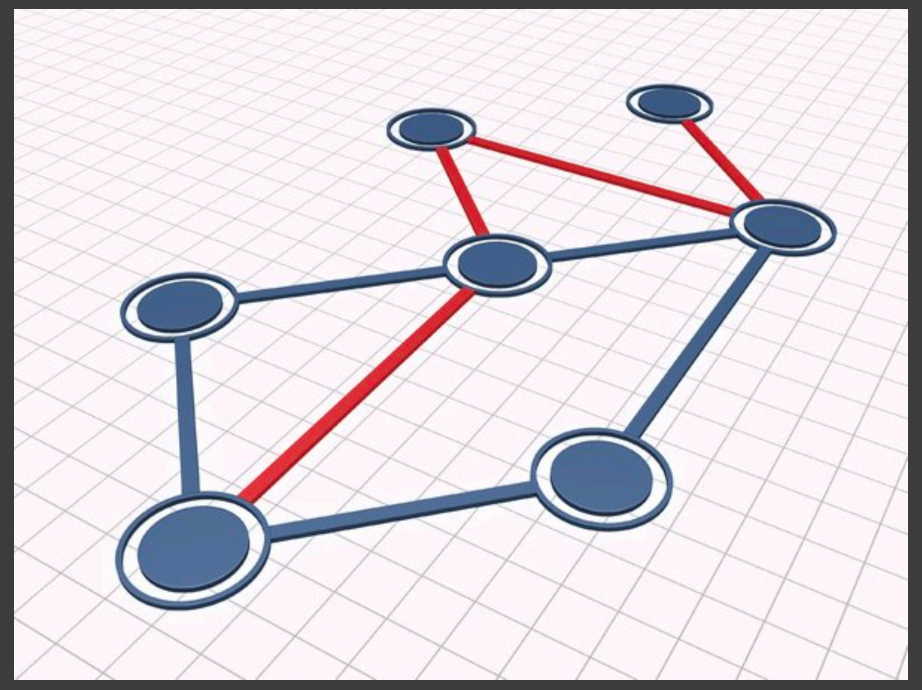
Mitchell Stern
mitchell@berkeley.edu
University of California, Berkeley
Berkeley, California, USA

Course Wrap Up 🎉

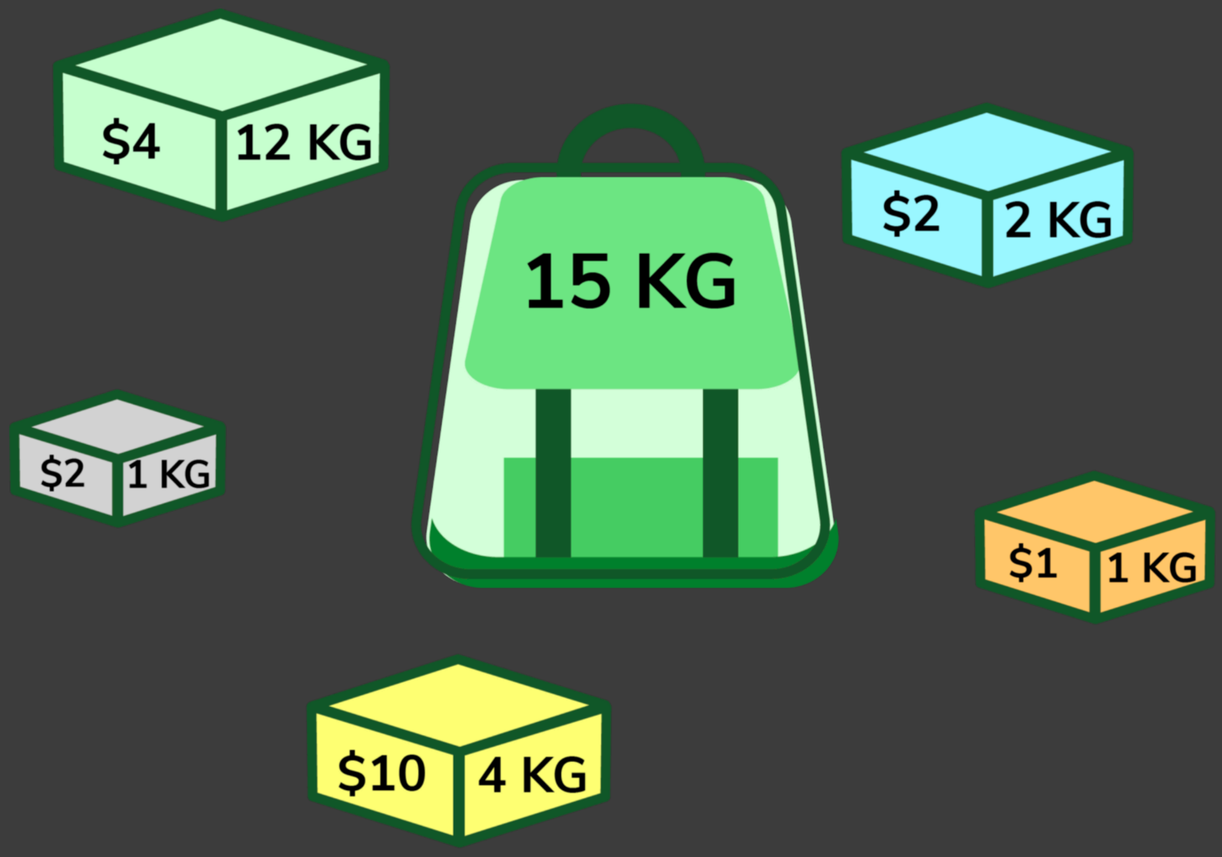
Algorithmic Game Theory

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

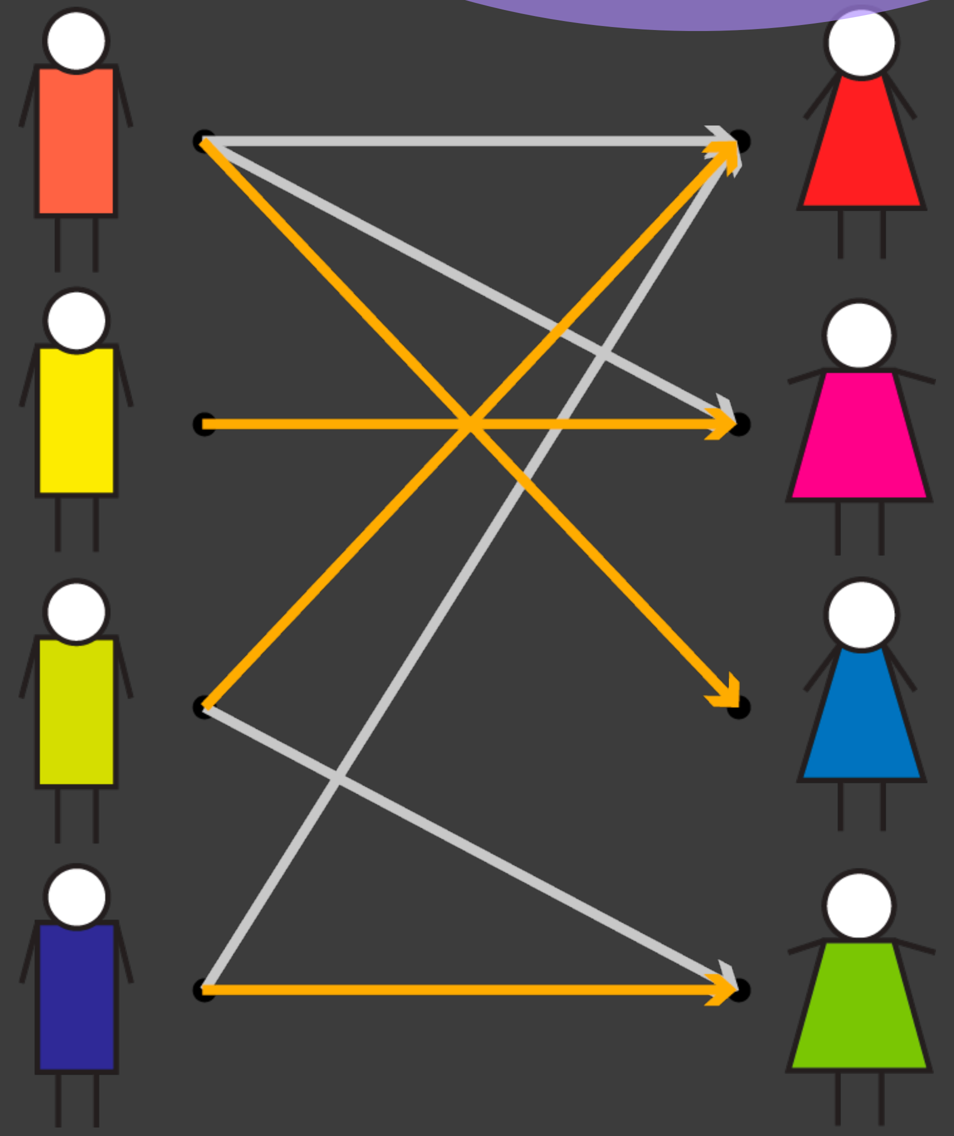




Routing in Networks



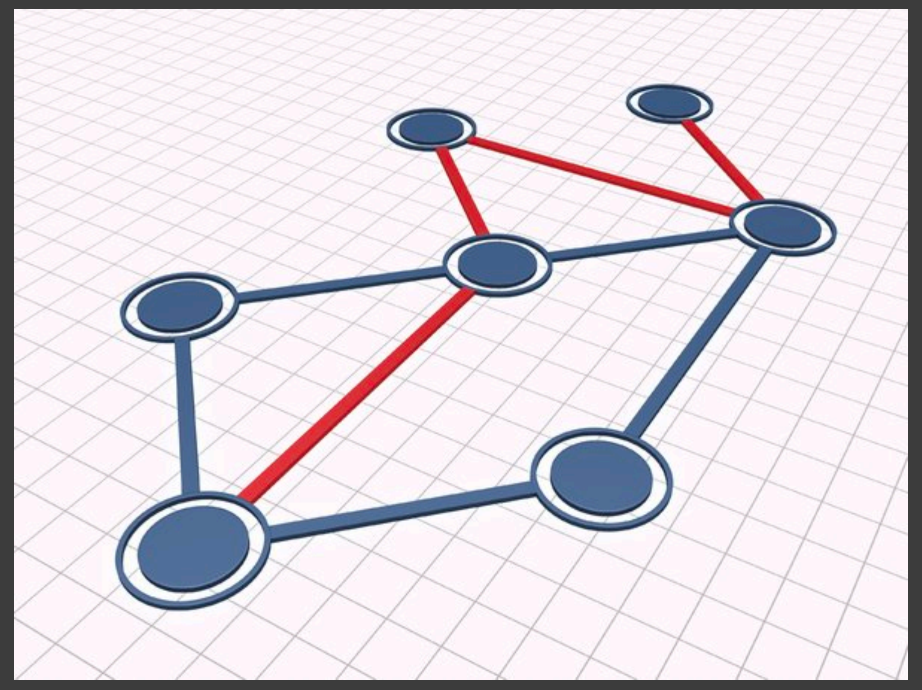
Resource allocation



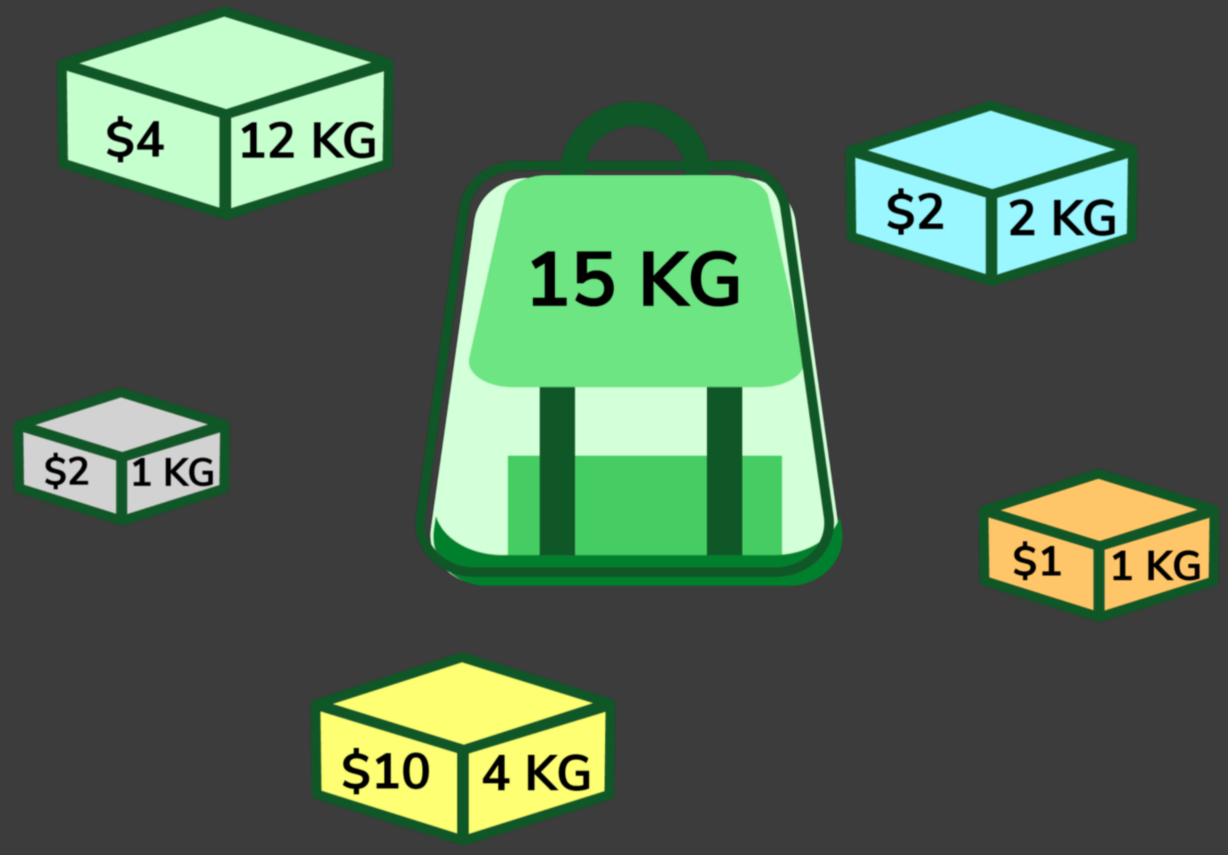
Matching problems

Algorithmic Game Theory

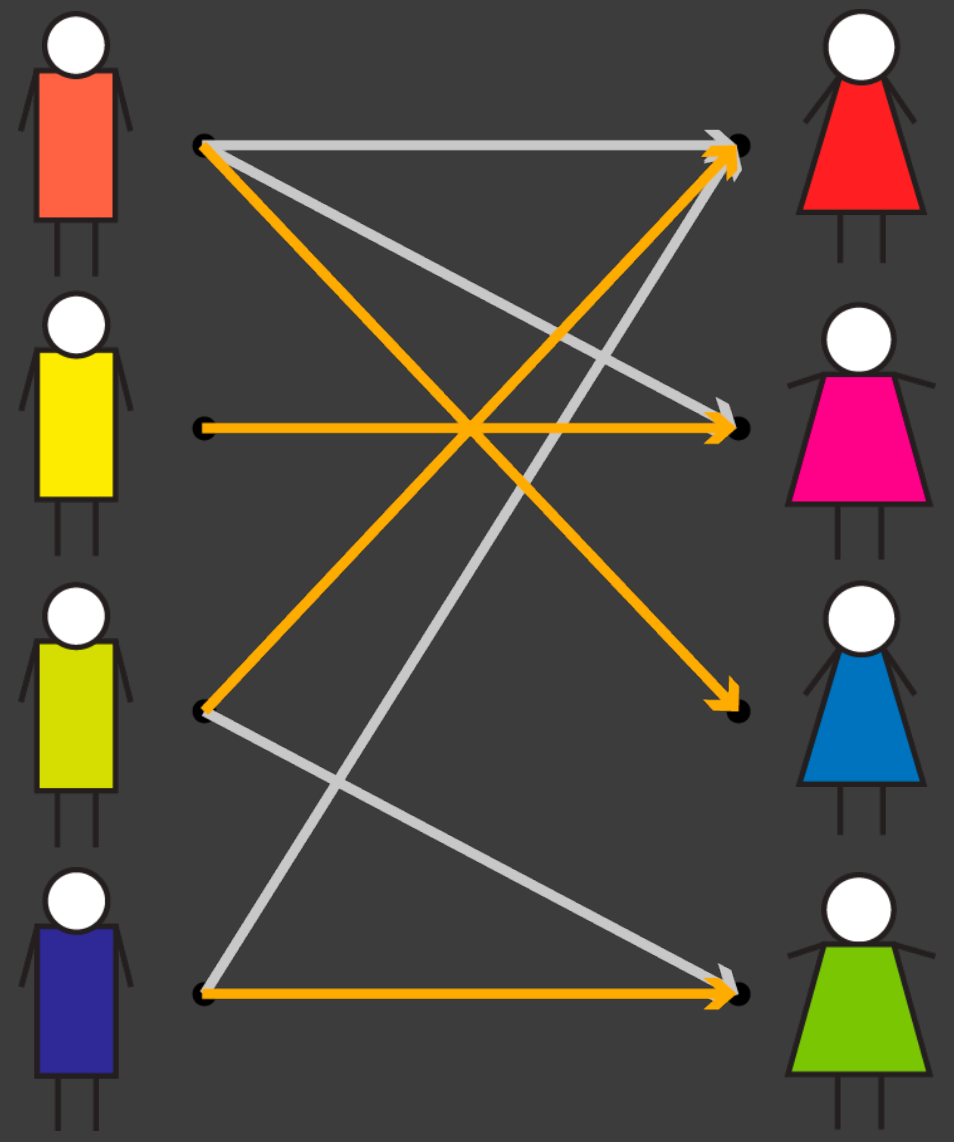
Often the system designer's (global) objective does not necessarily align with that of the participants (local).



Routing in Networks



Resource allocation



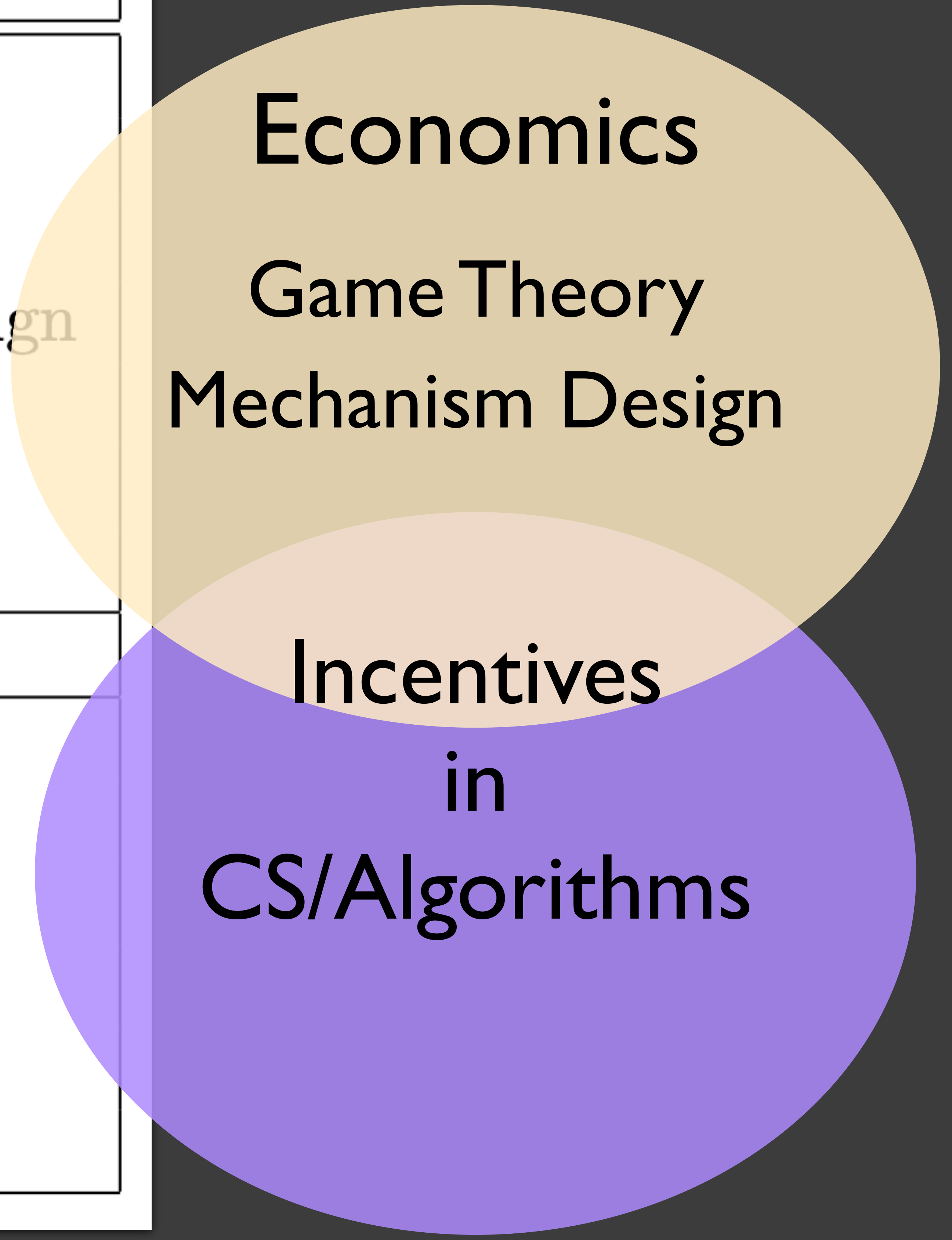
Matching problems

Algorithmic Game Theory: Topics

- Game Theory
  - Normal Form Games
  - Bayesian Games
  - Extensive-form Games
  - Repeated Games
- Mechanism Design w Money
  - Auction Theory
  - Matching Markets w Money
- Mechanism Design w/o Money
  - Matching Markets w/o Money
  - Social Choice & Voting
- Incentives in CS
  - Incentives in BitTorrent
  - Incentives in Network Routing
  - Incentives in Cryptocurrencies

Course Plan from Day 1

Week	Monday	Thursday
2/2	—	1. Welcome
7/2	2. Game Theory I	3. Game Theory II
14/2	4. Auctions I	5. Auctions II
21/2	6. Sponsored Search Auctions	7. Algorithmic Mechanism Design
28/2	8. Incomplete Information Games	9. BNE in Auctions
7/3	10. Revenue Maximization	11. Matching Markets
14/3	12. Stable Matchings 1	13. Stable Matchings 2
	Spring Break	Spring Break
4/4	14. Top Trading Cycles & Kidney Exchange	15. Voting 1
11/4	16. Voting 2	17. Sequential Games
18/4	18. Repeated Games & BitTorrent	19. BGP Routing
25/4	—	20. Spectrum Auctions
2/5	21. Incentives in Blockchains	22. Complexity of Equilibrium
9/5	23. Project Presentations	24. Project Presentations



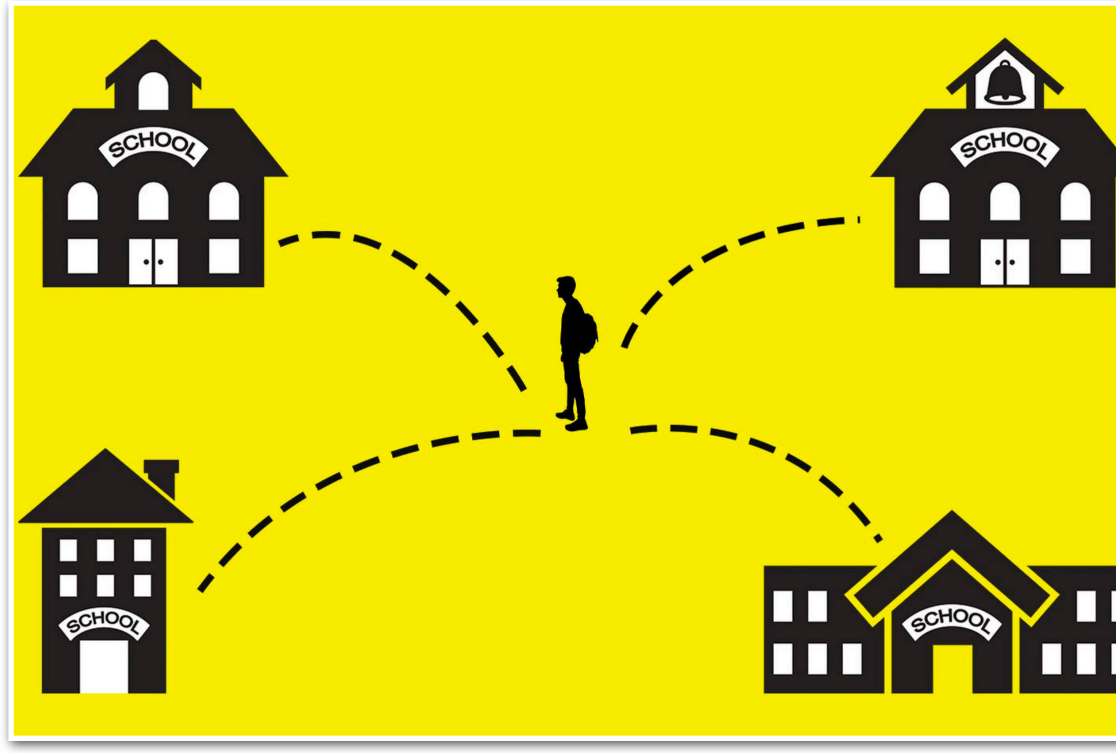
Game Theory: Equilibria

- How bad is selfish behavior (what's good for the one) for the group?
- We analyzed selfish behavior through "solution concepts"
  - Dominant strategy equilibrium
  - Nash equilibrium
  - Bayes' Nash equilibrium
  - Subgame perfect equilibrium
- Complexity of finding equilibrium
- Performance guarantees of equilibria: price of anarchy

Mechanism Design (with Money)

- Mechanism design: How to design the game such that the equilibrium behavior is what we want: e.g., truthfully reporting values/perferences
- With money (mechanism design through auctions and VCG):
  - Studied many fundamental results with a unified theory
  - **Auction Applications**:   sponsored search auctions, spectrum auctions, decentralized markets
  - Auction theory is now being applied to decentralized digital currency markets: how to charge transaction fee?

Mechanism Design (w/o Money)



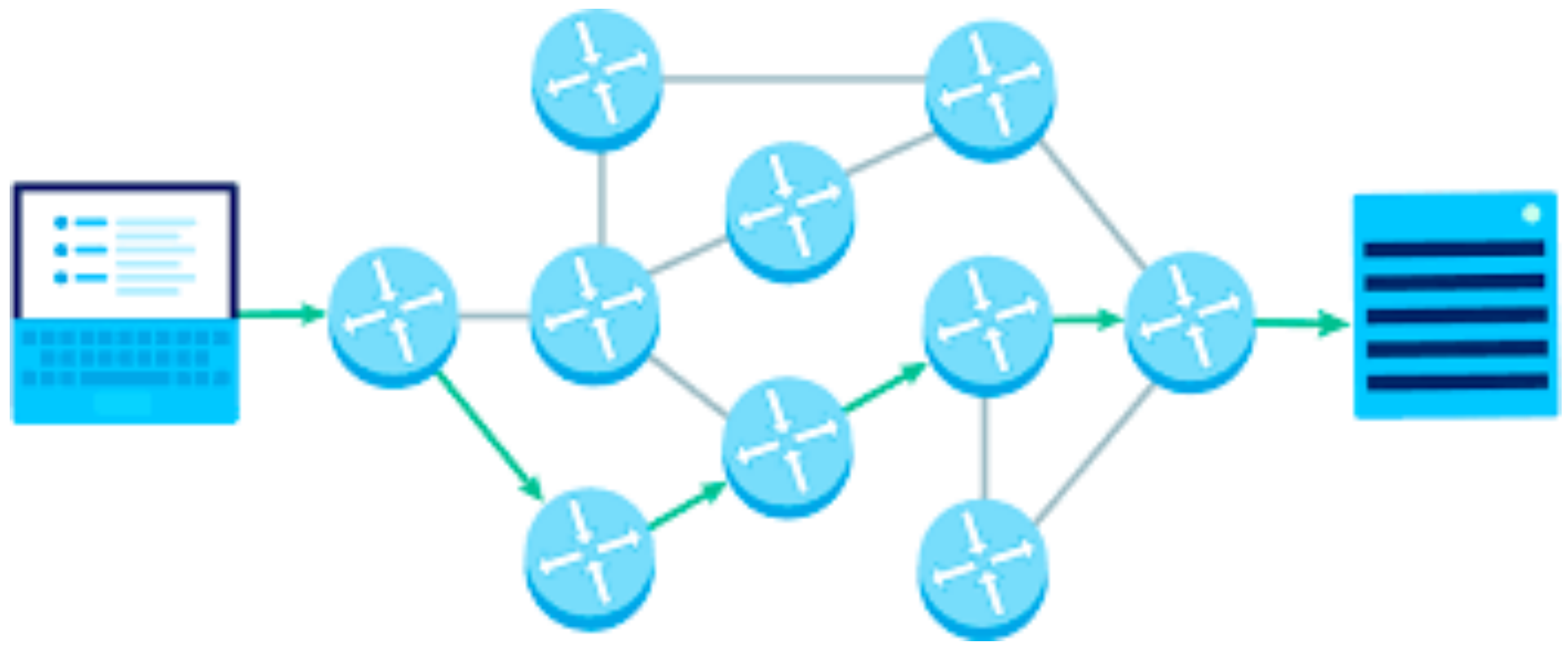
- Matching markets
  - One sided or two sided
  - Applications: dorm assignment, course assignment, matching students to residents, kidney exchange, school choice
- Voting and social choice:
  - Which voting rules are good and why?
  - Gibbard-Satterthwaite theorem and ways to circumvent it
  - Fair division

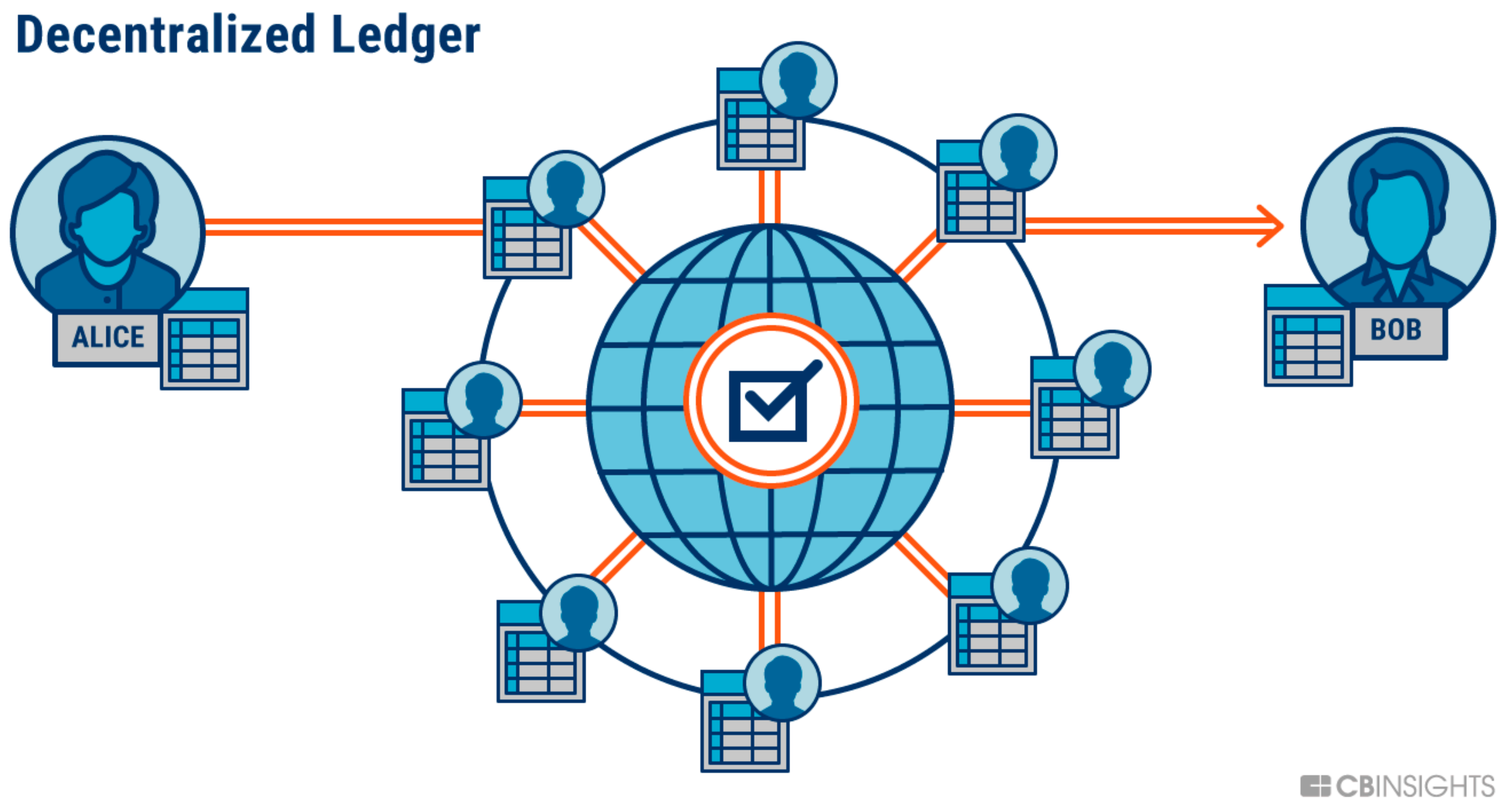
Incentives in P2P

Do these AGT lessons apply to computer systems?

- Networks: Analyzing selfish behavior explains why (slight) over-provisioning in computer networks significantly improves performance
- Incentives in P2P systems such as file sharing (torrents), BGP routing, blockchains, etc.

BitTorrent™

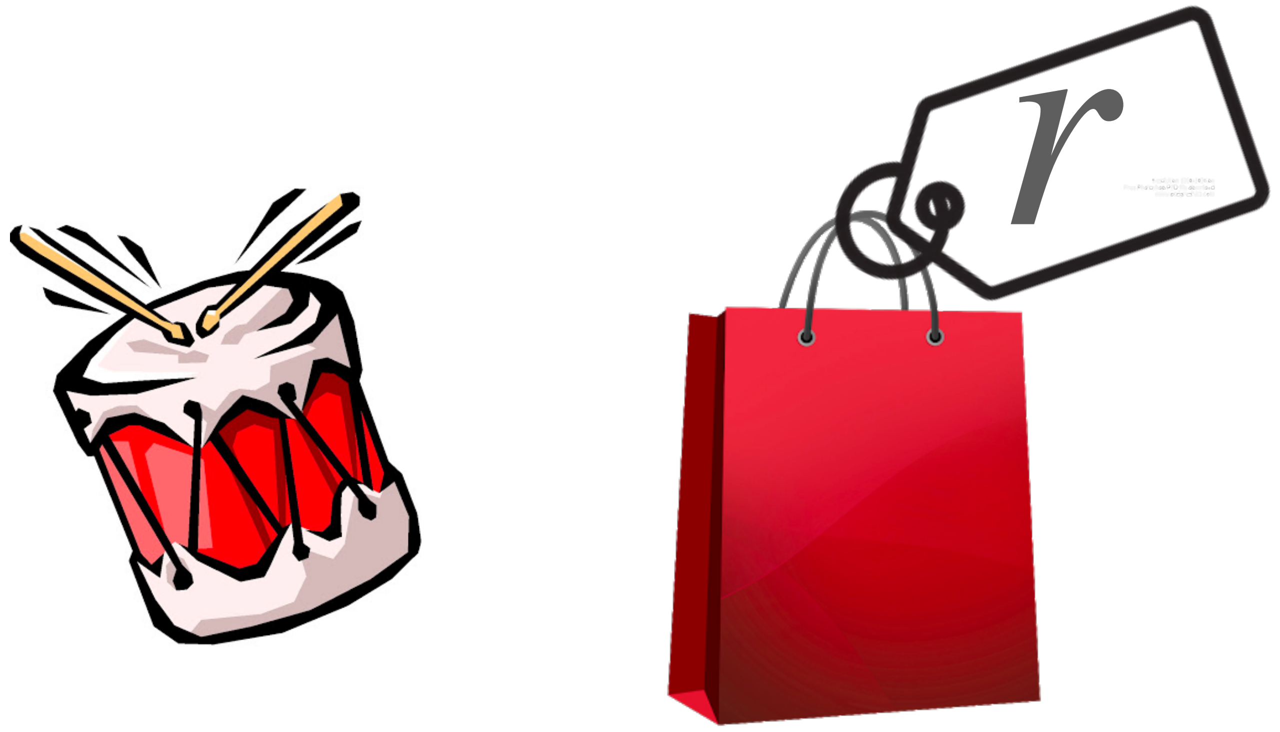




Cocktail Napkin Stories

Prisoner's Dilemma

Revenue Equivalence

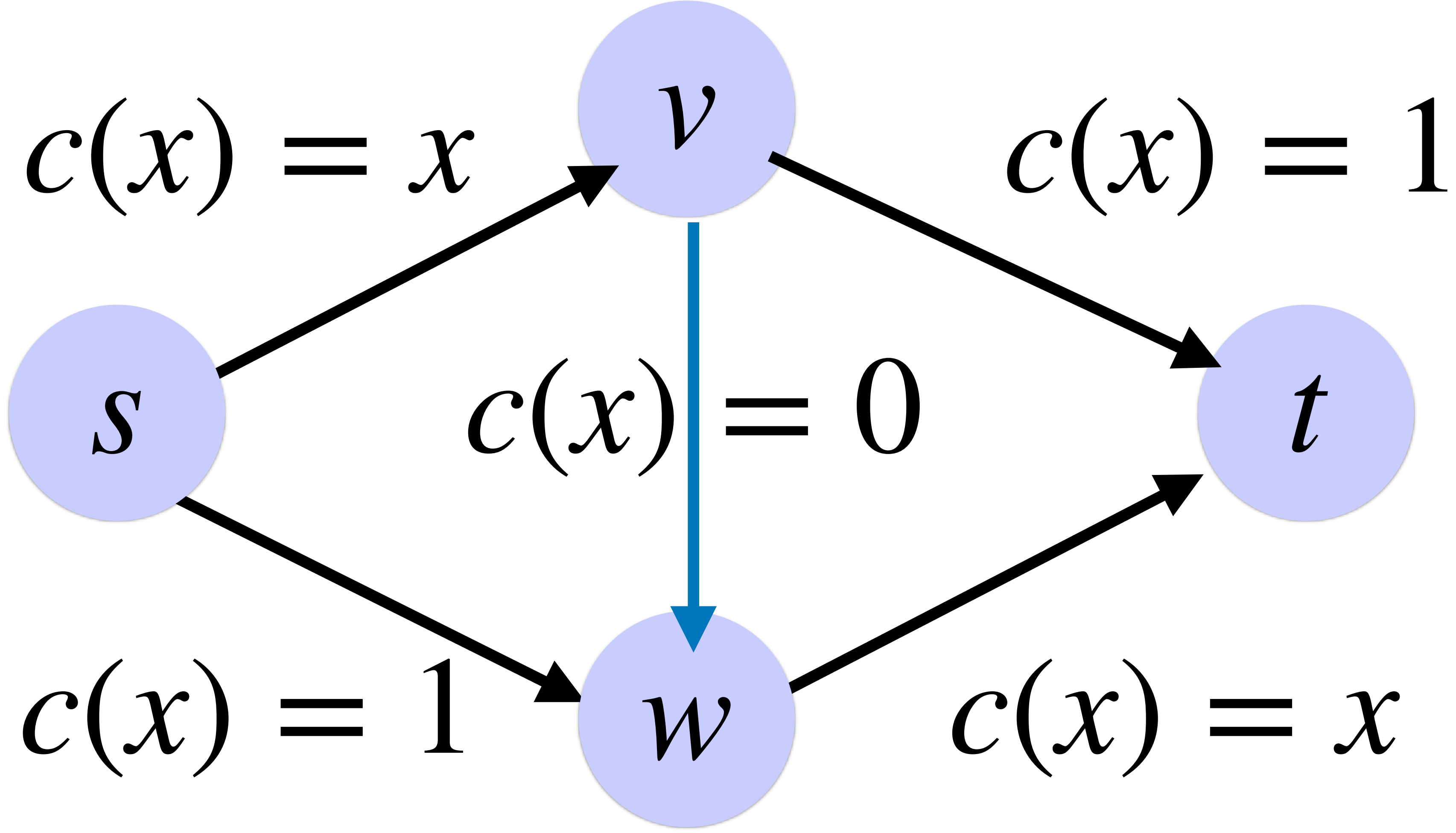


2/3rds Game

Envy-free Cake-cutting!

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

Braess Paradox



The AGT Mindset: Rules Matter!

- There are 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

Course Evals Logistics

- 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 tenure/promotion & seen by CAP etc, **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.*

Acknowledgments

- These lecture is partly based off the following:
    - http://timroughgarden.org/f16/l/l9.pdf
    - Chapter 21, Parkes and Seuken

Credit: Roughgarden