14.129
Spring, 2025
Blockchain and the Design of Financial Systems

Lecture 1

Introduction to the Class

Robert M. Townsend

Elizabeth & James Killian Professor of Economics, MIT

Massachusetts Institute of Technology

Introduction to the Class

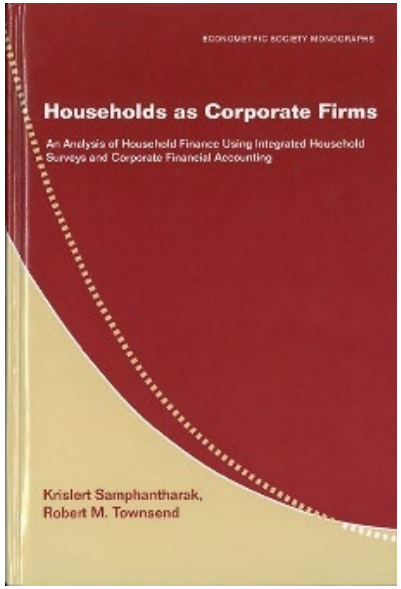
- Course 14.129 will synthesize the computer science technologies underlying cryptocurrency, blockchain, tokenization, platforms, and computational algorithms with the economics tools of contract theory, mechanism design, general equilibrium theory, and monetary theory.
- The goal is to understand the assumptions and existing shortcomings of distributed ledgers, smart contracts, and encryption, and potential impact of these technologies on legacy systems
- And to explore possibilities for new financial designs and for regulation
- Each lecture, or cluster of adjacent lectures, features one or several of the computer science technologies in the context of historical and contemporary economic applications, using the various economic tools.
- Example applications and topics include: Community currencies, coordination and financial crashes, tokenized assets and trade fails, multilateral payment and trade credit setoffs, liquidity injections and financial contagion, risk sharing, auctions, and on-line markets.

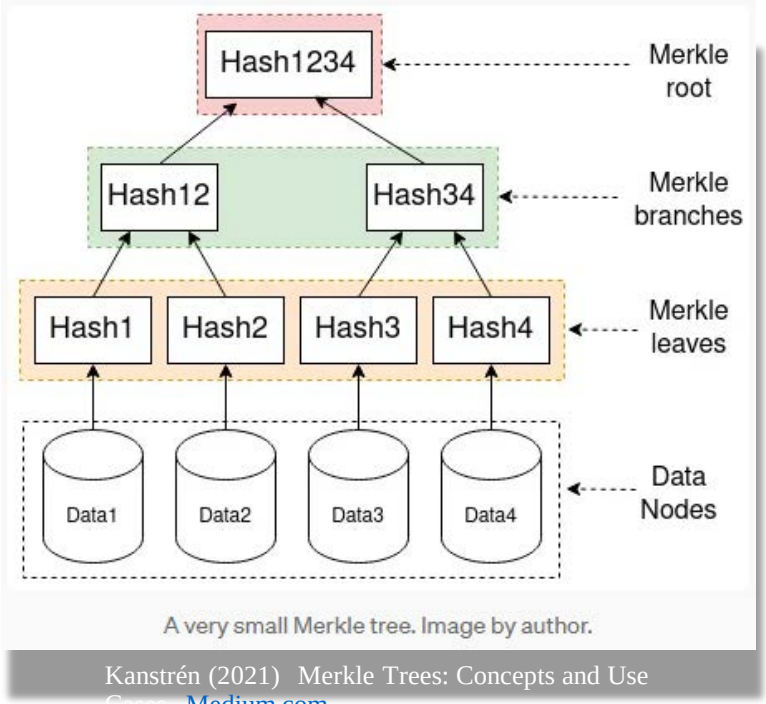
Introduction, continued

- Emphasis is given to unpacking the different computer science technologies and assumptions, sometimes rearranging them, rather than accepting conventional bundles and labels.
- For example, one can combine the authentication and commitment schemes of encryption with an automated execution engine on a distributed ledger but also do so with computer code without a consensus algorithm, or even with trusted third parties operating escrow accounts.
- Related, different technologies allow different implementations of the "central planner" construct of economics and gradually abstract this centralized role away in concretely deployed mechanism designs and commercial applications.
- The goal is a balanced perspective, avoiding hype and ideological positions, focusing instead on ways to implement use cases in various economic contexts, allowing policy designers to leverage technological tools for the different problems they are facing.

Lecture 2: Blockchain as a Database

- Longer Title: A Unified View of Distributed Ledgers and Financial Accounts as Data Bases, Distinct Views of Money, the larger Community perspective.
- Blockchains and financial accounts are each a database of transactions, best viewed from a unified perspective
- Association with money
  - For the blockchain: crypto currency
  - For financial accounts: a particular item the balance sheet of the holder (alternatively, a particular liability of an issuer)
- But each is broader





A very small Merkle tree. Image by author.

Kanstrén (2021) Merkle Trees: Concepts and Use Medium.com

Lecture 2, continued

- For blockchain and financial accounts, both can incorporate multiple objects.
  - The monetary theory definition of money is an object (good, asset, certificate) that appears frequently in exchange
    - As in a matrix of transactions
    - Or having high velocity, average amount traded per unit time divided by stock outstanding
  - There can be multiple objects serving as such a money and some not-monies
- Blockchains as a way to write and execute contracts, generalize the balance sheet and transfers to states and state changes
- The individual vs. community perspective is telling
  - For financial accounts, money of the holder is an asset but a tension in operations, between money as store of value and as medium of exchange.
  - In its original formulation, the community blockchain perspective was dominant: In double-entry bookkeeping, money is a liability, to be returned to the community as part of a larger purpose
- Technological limitations to blockchain and related trilemmas
  - CS, the CAP theorem
  - In actual entire economies, what are the ways in which data systems are fragmented?
    - Local for trust, intermediary balance sheets, CSD
  - How to engineer improvements? Progress in mapping economies

Village India: Money, IOUs, Grain

TABLE III
Exchange Matrix for Aurepalle Village[a]

Goods or services out	Goods or services in (value percent)													
	Money	IOU	Grain	Other crops	Food other than crops	Clothing	Other consumptions	Labor	Livestock	Physical assets	Jewelry	Consumer durables	Inputs	Others
Money	·	8.22	2.92	4.99	0.17	1.52	3.87	0.83	2.56	2.69	0.55	2.91	2.30	3.60
IOU	10.00	0.02	0.93	0.20	0.01	0.42	0.15	0.06	0.31	·	0.37	0.24	0.05	0.04
Grain	2.34	2.90	0.04		0.00	0.00	0.03	4.52	0.02	·	·	0.01	·	0.02
Other crops	6.49	0.74	0.00	0.02	0.00	·	·	0.18	0.05	·	·	·	·	0.01
Clothing	·	0.31	·	·	·	·	0.02	0.00	·	·	·	·	·	·
Other consumptions	0.02	·	0.01	·	·	·	·	·	·	·		·	·	·
Labor	1.40	·	4.56	0.16	0.01	0.00	0.00	0.02	0.00	·	·	0.00	·	·
Livestock	3.25	0.16	0.00	0.03	·	·	0.01	0.00	0.22	·	·	·	·	·
Physical assets	6.05	0.49	0.03	·	·	·	·	·	·	·	·	·	·	·
Jewelry	1.09	0.05	·	·	·	·	0.23	·	·	·	·	·	·	·
Consumer durables	0.45	0.23	·	·	·	·	0.02	·	·	·	·	0.06	·	·
Other	10.67	0.00	0.79	0.19	1.19	0.00	0.01	0.01	·	·	·	0.01	·	0.01

[a] 0.00 denotes a positive number which is rounded to zero. The heavy dot (·) denotes true zeros.

The Cap Theorem

CAP theorem Euler diagram

In database theory, the **CAP theorem**, also named **Brewer's theorem** after computer scientist Eric Brewer, states that any distributed data store can provide only two of the following three guarantees:[1][2][3]

Consistency

Every read receives the most recent write or an error. Note that consistency as defined in the CAP theorem is quite different from the consistency guaranteed in ACID database transactions.[4]

Availability

Every request received by a non-failing node in the system must result in a response. This is the definition of availability in CAP theorem as defined by Gilbert and Lynch.[1] Note that availability as defined in CAP theorem is different from high availability in software architecture.[5]

Partition tolerance

The system continues to operate despite an arbitrary number of messages being dropped (or delayed) by the network between nodes.

When a network partition failure happens, it must be decided whether to do one of the following:

- cancel the operation and thus decrease the availability but ensure consistency
- proceed with the operation and thus provide availability but risk inconsistency. Note this doesn't necessarily mean that system is highly available to its users.[5]

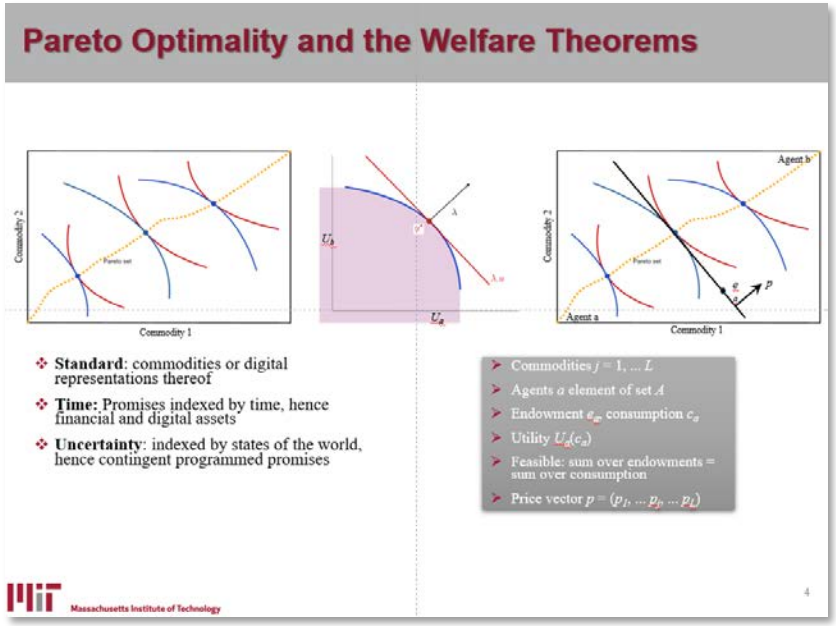
Wikipedia (2024) "The CAP theorem"

Readings and Research, examples

- Agustín Carstens (2023) “The future monetary system: from vision to reality” BIS.org
- The Baby-Sitting Economy: Krugman 1988 Journal of Money, Credit, and Banking in 1978, “Monetary Theory and the Great Capitol Hill Baby-Sitting Co-op Crisis” by Joan and Richard Sweeney.
- Goldstein et al (2023) “Payments, Reserves, and Financial Fragility”
- De Meijer (2023) “Sarafu: Crypto Currency for Rural Communities” treasuryXL.com

Lecture 3: Distributed Ledger as Solution to an Information Problem

- Longer Title: Fragmented Markets, Policy Objectives, Regulatory Solution, Distributed Ledger as Technology Solution
- Starting the with friction of fragmented markets, what is the problem and what criterion should be used to weigh potential remedies.



- From general equilibrium theory, a useful standard is Pareto optimality, achieved under Walrasian equilibrium. Possible to achieve in practice?
  - A regulatory standard as under the US National Marketing System implicitly aims for this: Marginal rates of substitution across goods/assets should be equated, i.e., common prices

Lecture 3, continued

- The impossibility of efficient decentralized exchange, guidance from theory
  - From Ostroy-Starr's theorem; achieving efficient exchange with pairwise quid pro quo trades, even at the correct Walrasian prices, is in general not possible when information is decentralized – "programmed traders"
  - Bilateral credits and debits to financial accounts are insufficient.
  - A community perspective is needed. A common but distributed ledger provides the requisite information centralization.
- Current institutional configurations are inadequate
  - Money, broker dealers, and trade credit
  - Solutions in the theory only under special circumstances
  - In practice suffer from problems: not liquidity saving, distortions from market concentration, and credit defaults

$$N_2 = N = \begin{bmatrix} 4 & -2 & -2 & 0 \\ -3 & 1 & 1 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}; B_2 = B = \begin{bmatrix} 0 & 2 & 2 & 0 \\ 3 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Lecture 3: Readings and Research, examples

- Thomas Ernst and Chester Spatt (2024) “Regulating Market Microstructure”
- Martin and McAndrews (2008) “An Economic Analysis of Liquidity-Saving Mechanisms” FRBNY Economic Policy Review
- Alcazar et al (2024) “Market Structure of Core Banking Services Providers” Federal Reserve Bank of Kansas City
- “Update on Tri-Party Repo Infrastructure Reform” (2015) Newyorkfed.org

Lecture 4: Smart Contracts as a Solution to a Coordination Problem

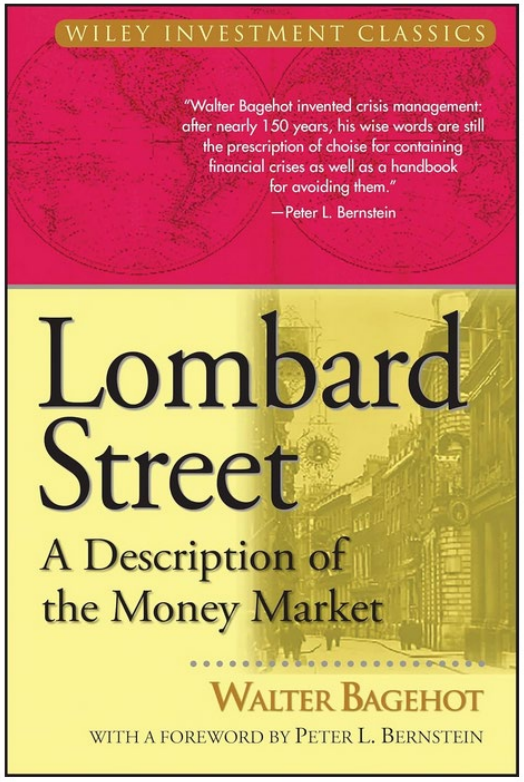
- Longer Title: Commodity Space with locations, dates and states, still the policy objective as Pareto Criterion; With Fragmented Markets, Implementation with Privately Issued Securities as Monies; Uncoordinated issues and Market Crises; Solution with multi-agent smart contract.
- Retaining market segmentation but now with explicit dynamics and 'agent max', the goal is to achieve efficient allocations in the space of locations and dates. With data, this provides policy guidance.
- Without explicitly complete initial markets, but with spot markets, agents can issue securities as promises to pay at designated locations and dates.
- In a competitive equilibrium, such private securities will circulate as monies among third parties, that is, appear frequently in exchange and have high velocity. These assets intermediate across agents' intertemporal budget constraints.

Table V-1. Who Meets Whom When

	Location	
Date	1	2
1	(1,2)	(3,4)
2	(1,3)	(2,4)
3	(1,2)	(3,4)
4	(1,3)	(2,4)

Lecture 4, continued

- However, a problem appears in the form of multiple equilibria. Various combinations of these circulating assets achieve the desired outcome, but agents in informationally decentralized locations cannot know what to issue and how to plan to trade.
- Without such coordination, there will be market crashes, clear from the theory, arguably observed historically, London money markets.
- A concern of low and middle income countries with the emerging digitization and e-money if there is not guidance.
- The solution is a cross location multi-agent smart contract written on Ethereum/EVM.

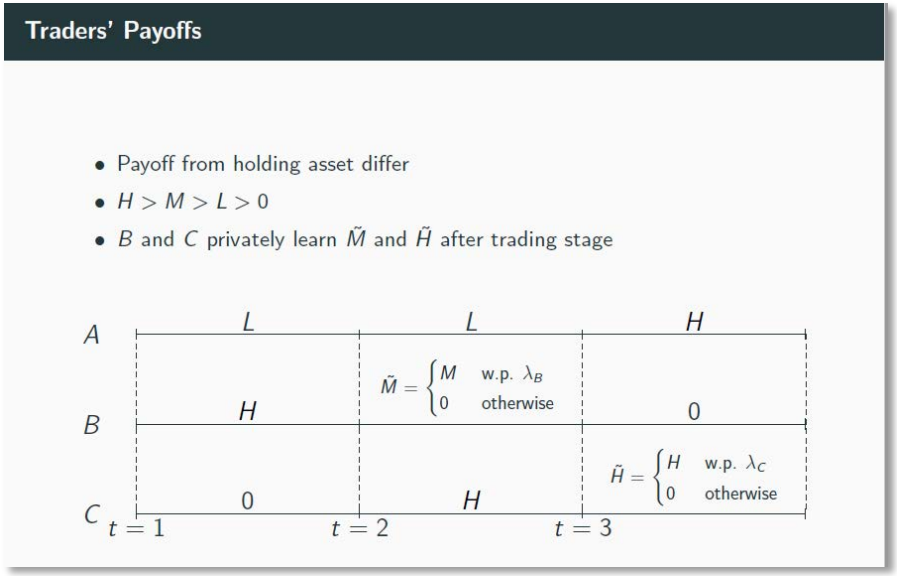


Lecture 4: Readings and Research, examples

- Guvenen, Schulhofer-Wohl, Song, and Yogo (2017) “Worker Betas: Five Facts about Systematic Earnings Risk” AER
- Gorton (2020) “Inland Bills of Exchange: Private Money Production without Banks”
- Bagehot (1873) “Lombard Street: A description of the Money Market”
- Sargent and Wallace (1982) “The Real-Bills Doctrine versus the Quantity Theory: A Reconsideration”
- “What Is Liquidity Fragmentation and Why It’s Killing DeFi” (2024) Medium.com

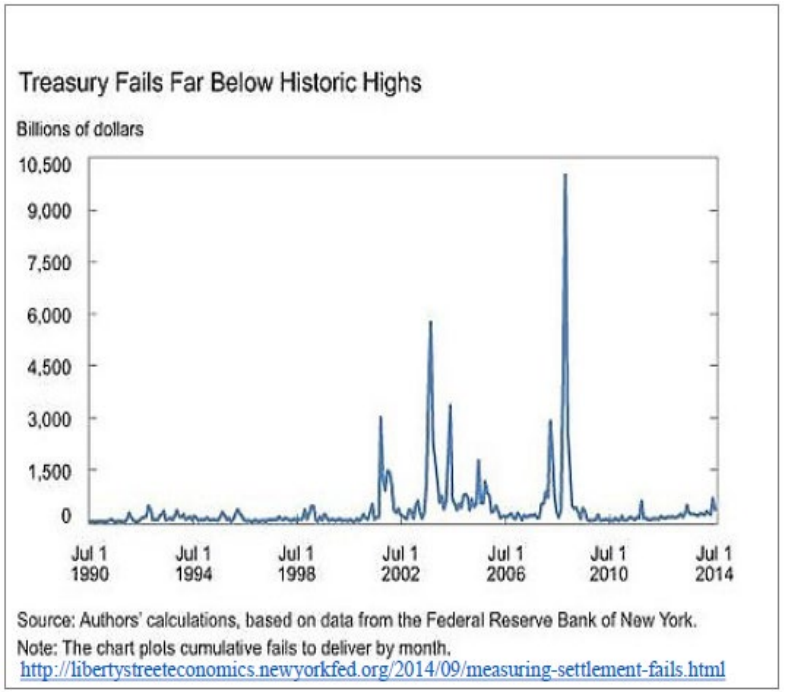
Lecture 5: Tokenized and Programmable Assets

- Longer Title: Dynamic Ledgers, Atomic Trade and Settlement, Platforms Legacy Systems, and Trade Fails
- Tokenization and programmable assets under multilateral smart contracts are key innovations made possible by CS
- When translated to legacy systems, these may seem alien, at first
- First, the balance sheets of financial accounts are not simply static snapshot pictures at various points in time.
  - Rather the ledgers themselves are dynamic, a representation of assets in possession over explicit dates (and states)
- Second, though contracts and trades are agreed at initial dates, and executed at subsequent dates, with programmed assets, trade and settlement are instantaneous (atomic)
- Thus there are no trade fails, in which either money or assets are not delivered, and there is no need for buffer stocks



Lecture 5, continued: Trade Fails

- New tech as remedy for trade fails, but there can be drawbacks
  - In fragmented markets in which broker dealers as intermediaries play key roles
    - If an asset can only be programmed by someone in possession of it, without the functionality of conditional release, entering into trade can reveal private information and result in a hold up problem
    - Solutions lie with more centralized markets and with encryption
- Such systems may be only partially interoperable
  - And interacting with legacy assets can raise issues of trust
- International agencies and domestic central banks are proposing, and constructing, platforms
  - The IMF proposes a cross border exchange and contract platform for FX transactions, segregated from domestic systems, apart from tokenization of central bank reserves
  - The BIS proposes a unified ledger even for domestic systems, for exchange and contracting, arguing for tokenization of some but not all assets, though a coherence guarantee is needed for consistency



Lecture 5: Readings and Research, examples

- Fleming and Garbade (2005) "Explaining Settlement Fails" NewYorkFed.org
- BIS Committee on Payments and Market Infrastructures (2019) "Wholesale digital tokens" BIS.org
- Lee (2021) "What is programmable money?" FRB Board of Governors
- PROJECT Helvetia phase 2, SNB Swiss National Bank and SIX Swiss Central Securities Depository
- Fnality Global Payments (consortium of large banks); Euroclear Payments and Security Settlement using DLT

Lecture 6: Algorithmic Flows on Networks as Solution to Multilateral Settlement Problems

- Longer Title: Improving Financial Infrastructure; Network Cycles and Chains; Algorithms to Maximize Timely Payment with Multilateral Trade Credit Offsets
- Minimize the balance sheet impact of repo with mutualized credit default guarantees (the setting of US monetary policy)
- An obligation matrix specifies bilateral obligations over all potential pairs of participants.
  - For each pairing of agents i, j, the matrix registers the amount i owes j, or the reverse, or nothing.
  - This is represented also as a weighted directed graph with edges connecting nodes on a network.
  - Ability of agent i to pay can depend on whether i has incoming obligations from other agents k, for example.
  - Agents may be indirectly connected in complicated ways

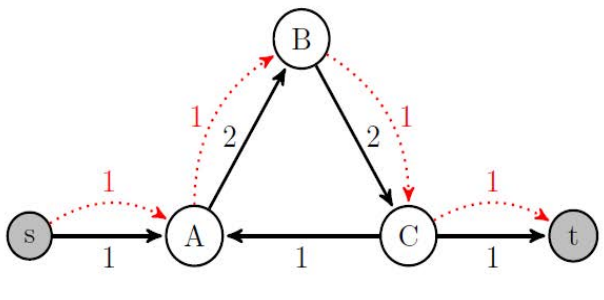


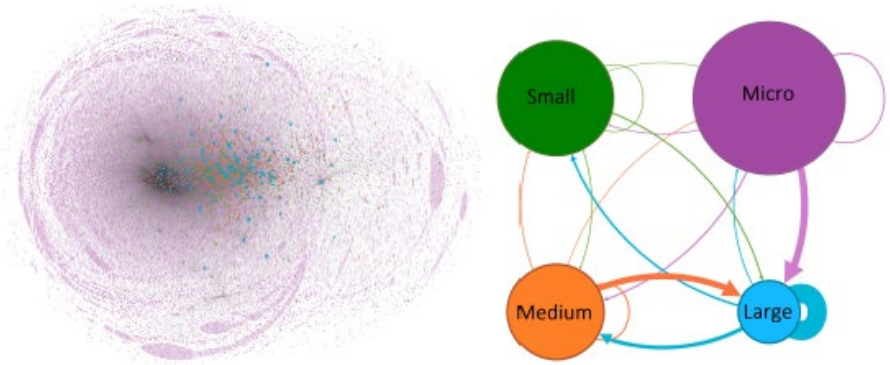
Figure 3: Balanced network representation with saturated flow from source (s) to sink (t).

Fleischman (2025) MTCS algorithm overview"

Lecture 6, continued

- This gives rise to a series of related problems
  - First, agents lack knowledge of the network, likely knowing only their own bilateral positions.
  - Second, arming a multilateral contract node with such knowledge, as a community ledger, still leaves to be determined the ordering of payments, and this is a combinatorial problem.
  - Third, if there were a liquidity pool or overdraft facility which could be used to maximize the amount cleared, to be decided still would be to whom to inject, what amount, and how to route to a collection point, so that the system remains balanced.
- These problems are typical, come up in a variety of contexts, and have costly economic implications when not solved
  - The featured problem is an overdue-trade-credit setoff problem
  - This is solved with an algorithm that maximizes flow through chains, as if from source to sink, leaving internal cycles which can be setoff
  - And employed on an actual large network
- A related problem: A chain of transactions among intermediating broker dealers, rehypothecation, which expands balance sheets and hit regulatory boundaries, limiting repo mkt
  - This is solved by a multilateral smart contract with mutual default guarantees

Figure 8: Network of trade credit claims



Lecture 6: Readings and Research, examples

- Fleischman, Dini, and Littera (2020) "Liquidity-Saving through Obligation-Clearing and Mutual Credit: An Effective Monetary Innovation for SMEs in Times of Crisis" Journal of Risk and Financial Management
- Cormen, et al. (2001) *Introduction to Algorithms*, Part VI, Graph Algorithms, chapters 21-25
- Aronoff and Townsend (2024) "A Trading Mechanism to Increase Intermediation Capacity in the Repo Market"

Lecture 7: Stochastic Financial Networks

- Longer Title: Liquidity and the Value of Key Players versus Contagion Dynamics: Enhance or Limit Markets
- Static network maps can be extended to dynamic stochastic maps, with edges linking nodes changing over time and with uncertain states.
  - At a given date and state, subclusters of nodes are directly or indirectly connected to each other.
- In a risk sharing problem, the income of nodes is randomly determined jointly with the network map.
  - The value of additional resources will vary with income and cluster characteristics.
- Suppose extra liquidity is available but must be injected ex ante, as with a new monetary policy
  - The problem is to determine which nodes receive liquidity and if so, how much
  - The subsequent flow among nodes in a cluster is determined by the cluster risk-sharing smart contract
- The value of nodes as injection sites can be determined
  - The most valued nodes are those that
    - participate in a market cluster when the number of active nodes is low
    - when there are aggregate and correlated income shocks
    - when average income is low
    - when agents in the cluster are risk averse

Example: Bech and Atalay (2010) - Federal Funds Markets

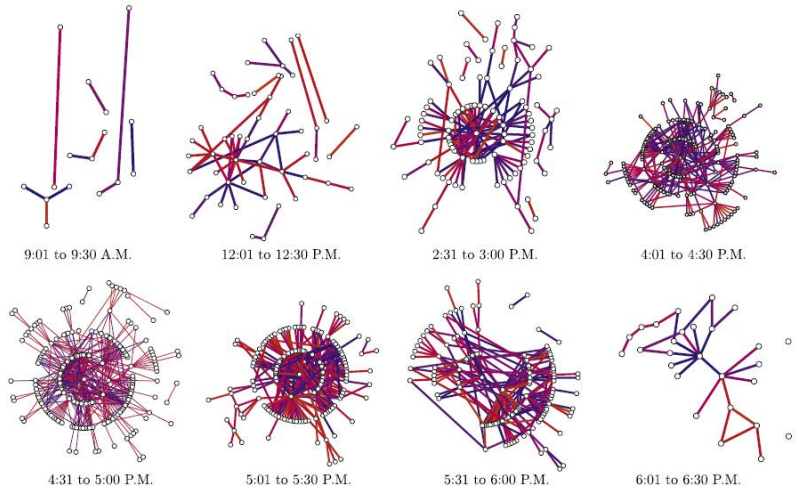
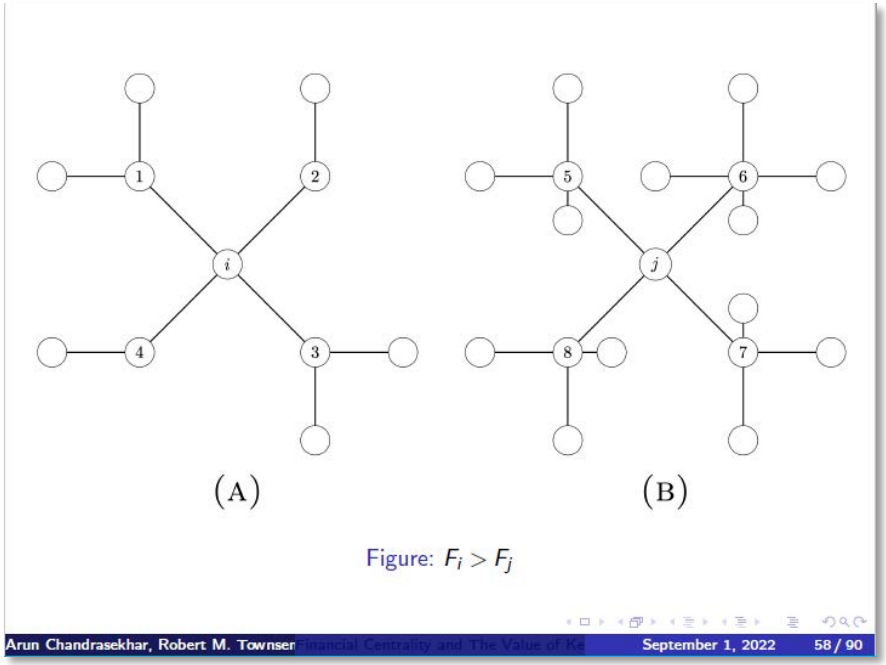


Figure: Federal funds networks at different times September 29, 2006

Lecture 7 continued

- Most valued nodes
  - In high valued financial markets the value of players is the price of a bond which pays off when that player is in the market.
  - In village settings, valued players receive more consumption on average as a premium received for insuring the others
  - Valued players are market makers
- In a literature on financial market contagion the logic is reversed
  - Adverse shocks (uninsured or unexpected) spread across nodes as a disease
  - Network centrality measures are used to guide regulation
  - Barriers are recommended to limit spread
  - Most valued nodes in the risk sharing formulation are not necessarily the most central nodes in the contagion literature

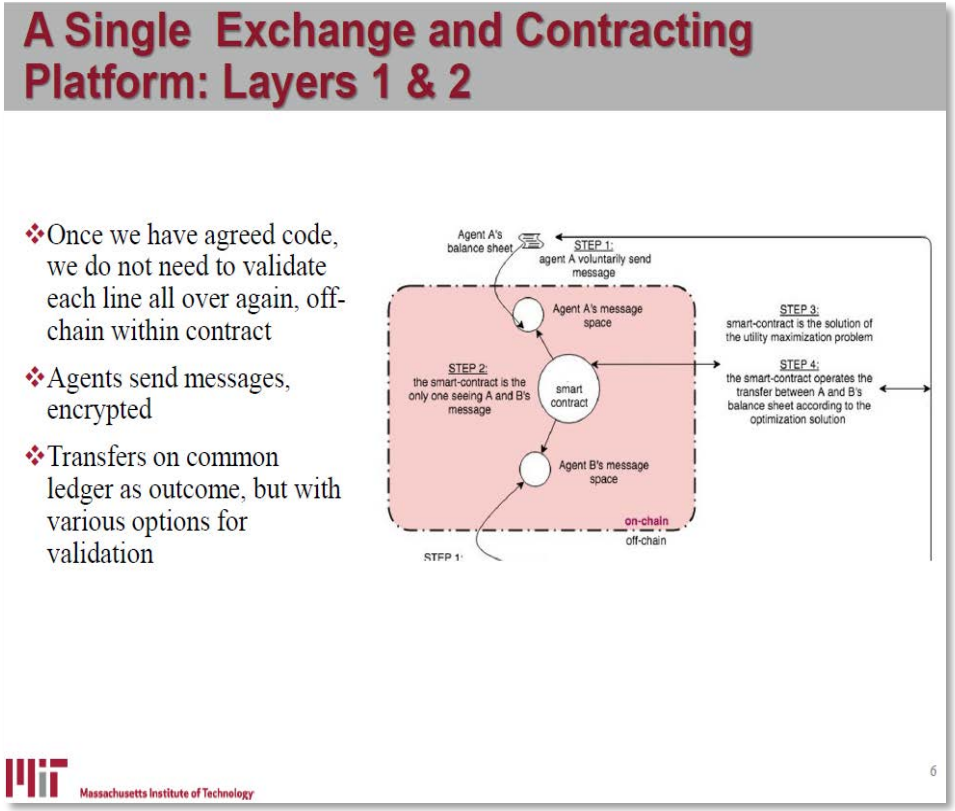


Lecture 7: Readings and Research, examples

- Hurd (2016) “Contagion! Systemic Risk in Financial Networks”
- Martin Sumner (2013) “Financial Contagion and Network Analysis” Annual Reviews

Lecture 8: Mechanism Design, Incentives vs Protocols, Notions of Trust

- Longer Title: Private Information, Incentives to Report and Take Actions, Byzantine Generals Problem, Differences between Economics and Computer Science approaches to Algorithms and Trust.
- With private information on hidden states and individual actions, as constraints, one can still characterize constrained-efficient allocations
  - Derive incentive constraints to report accurately and take appropriate actions
- An example: An agent that faces a loss with specified probability, with an insurance company prepared to at least partially cover the loss, but loss is private to the agent. Incentives can be given to report. Having multiple periods and tracking of the agents' history of past reports.
- Implementation would seem to require the trusted planner to be a real third party, but it does not.
  - Smart contract code can be validated by the agents in advance and hashed, a public commitment to carrying out the plan
  - Maximal payouts can be put in escrow as part of programmed dynamic contingent ledgers, as committed in advance, through tokenization and code
  - Messages can be recorded as part of the database associated with the contract
  - Implementation does not require implementation on a blockchain



Lecture 8, continued

- Blockchain validation protocols all rely on concept that computers and nodes can fail, and likewise that a rogue validator may not follow a protocol
  - Proof of Work, Proof of Stake, Byzantine Fault Tolerant
  - With postulated failure probabilities, one can tolerate deviations with sufficient numbers of computers or players
- But prescribed validation protocols are not necessarily incentive compatible in the sense of mechanism design
  - Agents will lie and deviate from the protocol if they have incentives to do so
  - There are strategic interactions among multiple players, with postulated outcomes captured by notions of Bayesian Nash equilibrium
  - The Byzantine Generals problem is illustrative

Table V. An equilibrium action protocol under the simple communication protocol.

State	Enemy's preparedness	Probability	First division general's action	Second division general's action
No message	Prepared	δ	Don't attack	Don't attack
Message sent but not received	Unprepared	$(1-\delta)\varepsilon$	Attack	Don't attack
Message sent and received	Unprepared	$(1-\delta)(1-\varepsilon)$	Attack	Attack

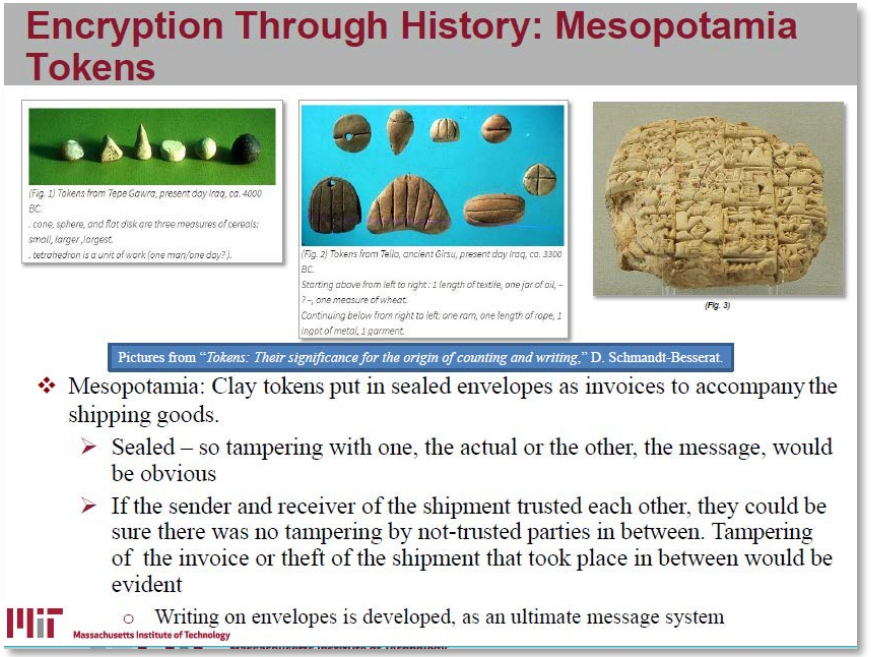
Morris and Shin (1997)

Lecture 8, Readings and Research, examples

- Sandholm (2008) “Computing in Mechanism Design” *New Palgrave Dictionary of Economics*
- Auer, Monnet and Shin (2021) “Distributed Ledgers and the Governance of Money” BIS.org

Lecture 9: Modern Encryption: Key concepts

- Longer Title: Public and private keys, encoded messages, hashes, cryptographic puzzles, fully homomorphic encryption, multiparty computation, zero knowledge proofs.
- Modern encryption is based on the principle that encrypted messages and also the way they are encrypted are both presumed to be public. Communication is secured by simply relying on the distinction between public and private keys.
- With these keys we can construct encoded message systems.
  - For incoming message Bob encrypts a secret message with that public key and send to Alice who can decipher it. Outgoing signed messages allow the receiver to verify the origin of the message (authentication), who sent it (sender non-repudiation), and that the message has not been modified (integrity).
- Hashes are a kind of signature system, a relatively short encrypted ciphertext which when deciphered links back exactly to an original document or data set for authentication or as indices for data storage to facilitate search.
- Cryptographic puzzles can be solved with a controlled level of difficulty, as with factoring prime numbers.
- Under fully homomorphic encryption (FHE) the true underlying space and its encrypted version are equivalent, so one can do addition and multiplication on ciphertexts and decipher the correct answer without seeing the inputs.



Lecture 9 continued

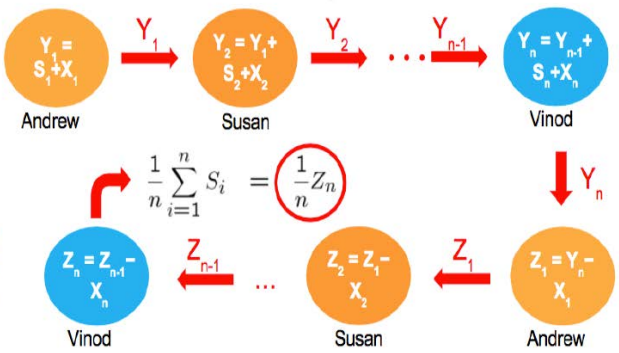
- The ability of agents to aggregate and make public the sum of secrets comes from multi-party computation (MPC)
- Zero knowledge proof (ZKP) is a version of signatures
  - For example, one can know that a message is reliable without ever seeing the underlying message

First Case, Privacy-Preserving Aggregation

- An illustration of "secure sharing" privacy-preserving aggregation

- On the right **s private data** *(ex line items on financial accounts)*

- x are random numbers chosen by each participant *(the x's can be seen as each agent encrypting his secret and then all agents collectively decrypting at the end)*



- NB: this back and forth *(2.n messages sent for one computation among n agents in this example)* is slow if every message sent has to be "validated" by **consensus**!

Massachusetts Institute of Technology 25

Lecture 9, Readings and Research, examples

- Canetti, Fiat and Gonczarowski (2023) "Zero-Knowledge Mechanisms"
- On zero knowledge proofs and interoperability see Chain Link, Layer Zero, Dfinity Internet Computer

Lecture 10: Designs of Financial Infrastructure Utilizing Encryption

- Longer title: Auctions, hybrid credit and insurance and implementation of cryptography on the block chain
- Auctions with private values, insurance with unobserved loss where histories are partially concealed, and order book matching as in decentralized markets can be formulated as mechanism design problems and implemented with encryption.
- Auctions can be run without a trusted third-party auctioneer.
  - The code can rank order bids as encrypted messages, and the mechanism selects the highest bid without knowing the bids, determining the winner.
- Insurance could cover relief from liquidity shocks to balance sheets, cash flow shocks to dealers or financial institutions, unobserved and kept private
- Information is decentralized in the sense that the information sets of the agents and what the code can infer are each distinct.
- Even requisite contingent randomization can be done with the code not knowing the underlying state.
- Past histories of messages are concealed to give high powered incentives.

Communication Concealed: Optimal Scrambling

Private Information Solution

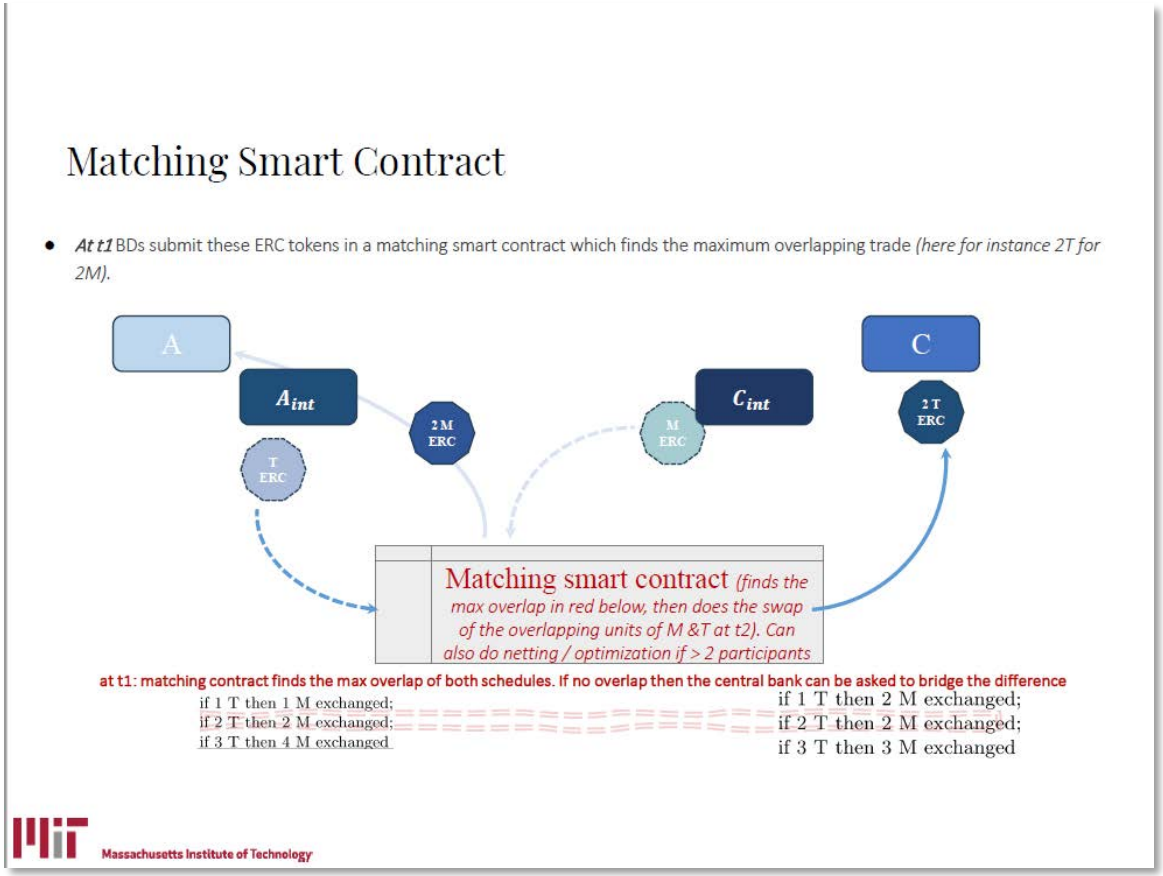
θ_0^a	(c_0^a, c_0^b)	$\pi(c_0, \theta_0^a)$	θ_0^a, θ_1^b	(c_1^a, c_1^b)	$\pi(c_1, \theta$
0.2	(1.75, 8.25)	1.0	(0.2, 0.2)	(4.75, 5.25)	1.0
			(0.2, 0.9)	(2.0, 8.0)	1.0
0.9	(0.0, 10.0)	0.1159346			
	(1.75, 8.25)	0.0339681	(0.9, 0.2)	(3.75, 6.25)	1.0
	(3.25, 6.75)	0.8544384			
			(0.9, 0.9)	(1.0, 9.0)	0.861060201
				(10.0, 0.0)	0.138397942

- The allocation $(c_0^a, c_0^b) = (1.75, 8.25)$ occurs with positive probability for either report of agent a
  - When $(c_0^a, c_0^b) = (1.75, 8.25)$ is observed, agent b remains uncertain of the type agent a reported in $t = 0$

Massachusetts Institute of Technology

Lecture 10, continued

- Under centralized matching, agents submit supply and demand functions, willingness to trade at various prices, all encrypted
- Encryption techniques are increasingly compatible with blockchains



Lecture 10, readings and research

- Bottazzi, Ngo and Tsutsumi (2024) "Multilateral Trade Credit Set-off in MPC via Graph Anonymization and Network Simplex"
- Chatzigiannis, Townsend, Aronoff, Zhang, Minaei, Raghuraman, and Bhat "SoK: Fully-homomorphic encryption in smart contracts"

Lecture 11: Implementing Market Mechanisms with Algorithmic Game Theory

- Longer title: Achieving Walrasian outcomes with computationally feasible algorithms, from Nash to Correlated Equilibria, to Course Correlated Equilibria
- Under Dubey's Price-Quantity Strategic Market Games agents can exchange goods by submitting limit orders that are then paired and exchanged between agents
  - The mechanism finds the competitive equilibrium of the market with favorable properties.
- Ramsayer et al designed a decentralized exchange (DEX), SPEEDEX, which similarly is a mechanism that facilitates exchange using limit orders
  - It does not contain any analysis on the economic efficiency of the market
- A goal is to bridge the gap between these two mechanisms, both computationally feasible and with efficiency properties.

Ramseyer, Goel, and Mazières (2023) SPEEDEX: A Scalable, Parallelizable, and Economically Efficient Decentralized Exchange USENIX.org

Lecture 11 continued

- The concern: With many agents and a continuum of price strategies to choose from, rational agents may not be able to find these equilibria.
  - The computational complexity for each agent to find their optimal strategy and submit bids in accordance with the noncooperative equilibrium is very large.
- An intuitive approach is to do some kind of computation that aims to find the noncooperative equilibrium and can then signal to the agents what their optimal strategy is.
  - To directly compute the noncooperative equilibrium takes worst-case exponential time to compute
- A correlated equilibrium is weaker than Nash and requires a central coordinator to pass signals to each agent to "coordinate" their actions. Coordinated equilibria can be found in polynomial time complexity using linear programming as well as machine learning techniques.

Readings and Research, examples

- Aumann (1974) “Subjectivity and correlation in randomized strategies” Journal of Mathematical Economics
- Papadimitriou and Roughgarden (2008) “Computing correlated equilibria in multi-player games” J. ACM
- Daskalakis, Goldberg and Papadimitriou (2009) “The Complexity of Computing a Nash Equilibrium” SIAM Journal on Computing

Final Notes

- Supplements to the lectures will be posted on the canvas site
- Course is tailored to individual student background and interests