CS61065: Theory And Applications of Blockchain

Welcome!

Department of Computer Science and Engineering

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Sandip Chakraborty
sandipc@cse.iitkgp.ac.in

Shamik Sural
shamik@cse.iitkgp.ac.in

Let's Start with an Example Scenarios ...

- Consider that Samir and Meera want to do a business transaction; Samir needs to transfer Rs. 14.52 Lakhs to Meera to make the payment
- Samir has an account at the State Bank of India (SBI), and Meera has an account at the Punjab National Bank (PNB)
- Samir initiates the transaction of Rs. 14.52 lakhs from his business account at the SBI to Meera's account at PNB
- SBI needs to transfer this money to PNB. How does SBI transfer that?

How do we do it today?

- Real-Time Gross Settlement (RTGS)

Deduct money from SBI ledger and add money to the PNB ledger

Other Examples of Centralization

amazon

Flipkart

6W 8 9GAG aftership AlikeAudience

bowtie dayta FinFabrik GreenTomato GRANA

GOGO VAN GOGOTECH haymarket InvestLab KeyChain Pay

KOPI Lively Impact LALAMOVE madhead mydress

QPT polljoy PIXELS Prenetics privé financial

RADICA SHOPLINE WeLend VYOND

eCommerce

Uber OLA

App Cabs

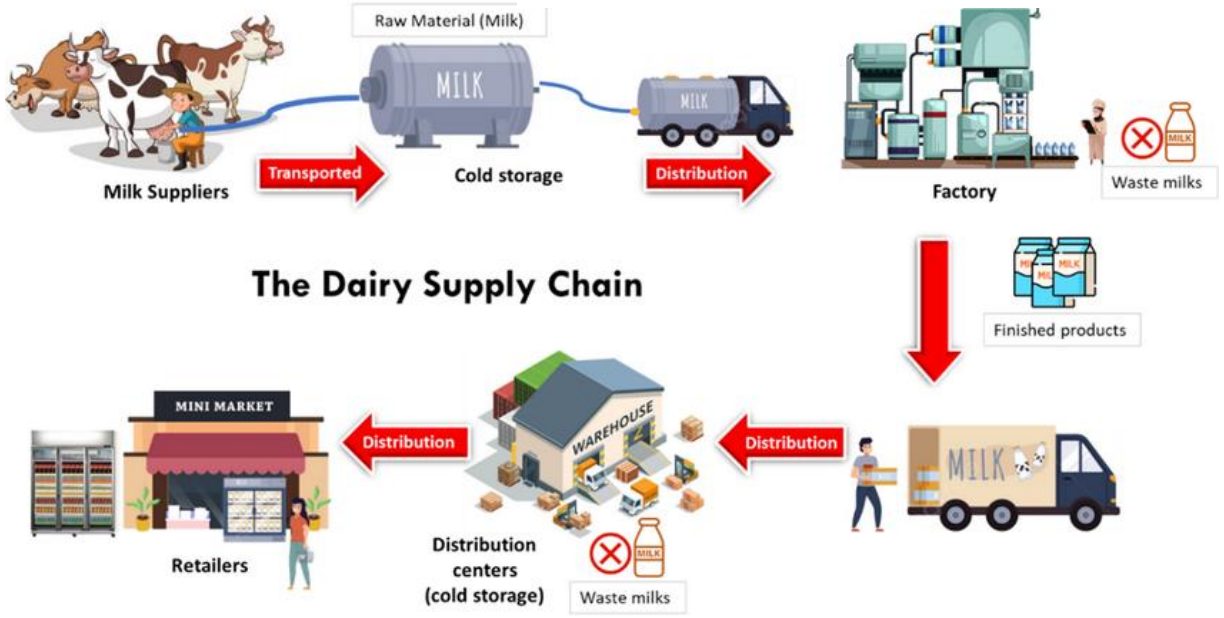
Centralization at the Supply Chains

Nestlé

Amul

DeHaat®
Seeds to Market

Cropin®



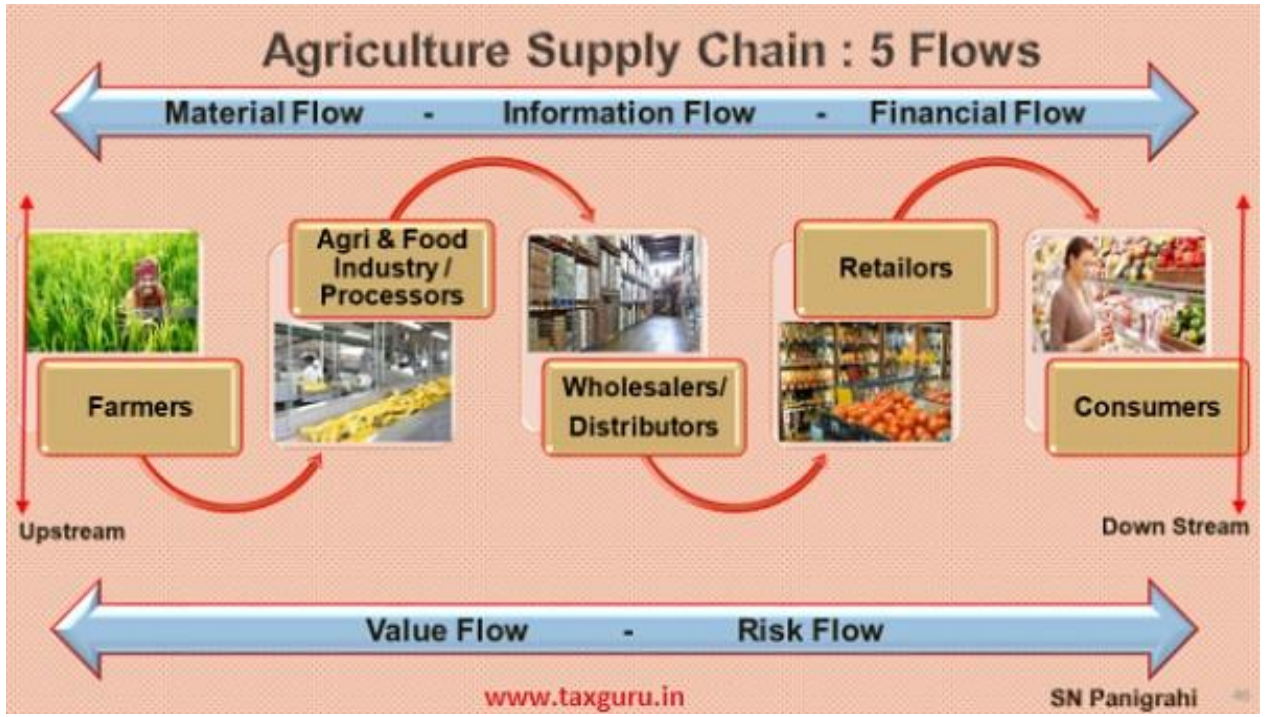


Image Source: http://dx.doi.org/10.1007/s41660-023-00382-3

Centralization has Its Own Advantages

Image Source:
https://theinvestorsbook.com/centralization.html

However, there are issues with centralization …

- **Inherent trust** on the central authority -- Can we trust them always?
- **Central point of failure** -- What if the central point fails (a DoS attack on the RBI network)?
- **Overhead** for the central authority -- Always need to cater to the peak load; waste of resources?
- **Auditing requirements** -- Auditing needs collecting the information from the central authority and tallying them with the stakeholder organizations
- **Transparency issues** -- The central authority decides what information they want to make public; may or may not be transparent to the stakeholders

And the news ...

Q & A

Inside the Brutal Business Practices of Amazon—And How It Became "Too Toxic to Touch"

In an interview with *Vanity Fair*, reporter Dana Mattioli reveals how the company systematically stifles criticism, squeezes out competitors, and even pits its own employees against one another. "People tend not to last," she says, "because it's very aggressive and it can be bruising."

TECH

Amazon has been promoting its own products at the bottom of competitors' listings

PUBLISHED TUE, OCT 2 2018•2:44 PM EDT | UPDATED MON, MAR 18 2019•3:48 PM EDT

Eugene Kim
@EUGENEKIM222

SHARE

KEY POINTS

- The new feature shows links to Amazon's own private-label brands inside rival listings.
- Amazon is aggressively pushing for the growth of its private label brands, which is estimated to generate $7.5 billion in sales this year.

FTC, 17 states sue Amazon for 'exploiting its monopoly power'

The e-commerce giant defended the practices outlined in the lawsuit, saying they "spur competition and innovation across the retail industry."

Published Sept. 26, 2023

Home | Business

Uber is basically promising investors it will become a monopoly

Oh goodie

TECHNOLOGY

Uber Fires Drivers Based On 'Racially Biased' Star Rating System, Lawsuit Claims

OCTOBER 26, 2020 · 3:47 PM ET

Bobby Allyn

The Notion of Decentralization …

- The similar businesses collaborate with each other to support the client services, without any steward or middleman

Ledger for financial transactions

A synchronization protocol to synchronize each cross-bank transactions

Ledger for financial transactions

The Notion of Decentralization ...

- The **similar businesses** collaborate with each other to support the client services, without any steward or middleman

Ledger for Driver-Passenger Mappings

A synchronization protocol to map each passenger request with a driver

Ledger for Driver-Passenger Mappings

However, there are challenges …

- Each business has their own **profit goals**
- The businesses are competitor to each other -- they **may not trust** each other
- Each business has their **own policy** which needs to be complied while making the transactions
- How can the **business disputes** be resolved?

Can we design a decentralized computing platform while mitigating the trust issues (the participants do not need to trust each other)

Decentralized vs Distributed

- Each decentralized system is also distributed by virtue, but not all distributed systems are decentralized!

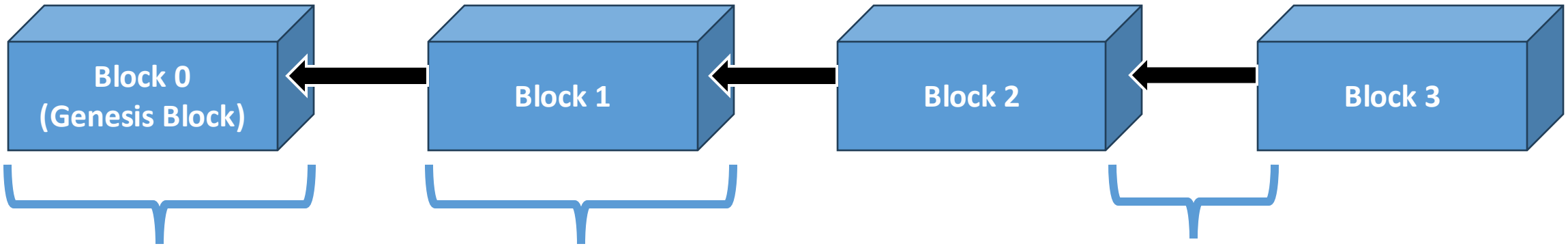
Decentralized	Distributed
The participants may or may not be uniform in terms of policies and organization management	The participants are typically unform; they have a common policy about data and management
The control for each organization is different; each manages their own control and policies	The organizational control is common, but the computing capabilities are physically separated and connected over a network
Example: Different banks doing the financial transactions across themselves	**Example**: The computing servers available over different branches of the same bank

Blockchain

- Blockchain enables us to develop **trustless and secured computation models** over decentralized architecture
- Also called **Distributed Ledger Technologies** (DLT)
  - Each organization maintains a copy (replica) of the shared ledger
  - Distributed computation models over the shared ledger to solve decision problems
    - What is the effective cash available at SBI?
    - Which driver will be allocated to a passenger?
    - Which products need to be displayed to an ecommerce customer based on the search request?
- Three pillars of blockchain or DLT
  - **Distributed Systems**: Builds up the backbone of the computation models (how to manage the shared ledger)
  - **Cryptography**: Ensures trustless and secured computation over the shared ledger
  - **Economic Models**: Designs incentive mechanism for the participants to join a network

What is a Blockchain?

- A digital representation of the shared ledger
  - Ensures **efficiency** in adding new transactions (added as a block; hence the term "*block*" in blockchain)
  - Ensures **security** of the transactions (subsequent blocks are connected, making it a chain-like data structure; hence, the term *"chain*" in blockchain)



The Generation and Management of the Ledger

- The basic operations on the ledger:
  - Read a transaction from a block
  - Add a new block in the ledger (after necessary verifications)
  - **Note:** We cannot delete an entry from the ledger; can you think why?

The Generation and Management of the Ledger

- The basic operations on the ledger:
  - Read a transaction from a block
  - Add a new block in the ledger (after necessary verifications)
  - **Note:** We cannot delete an entry from the ledger; can you think why?
- We need several **distributed protocols** to manage the ledger operations over a decentralized environment
  - Who can add a new block in the ledger?
  - When can a new block be generated?
  - How can we verify the correctness of the ledger blocks?
  - How do we ensure consensus in block generation (all the participants or at least the majority should agree upon the newly generated block)

About This Course ...

- You'll learn from the scratch on how to develop a blockchain-based system and use it for some specific applications
- Specific Topics:
  - History and Evolution of Blockchain-based Systems
  - The basic crypto primitives
  - Blockchain Data Structure, with a use-case of Bitcoin blockchain
  - Distributed consensus for blockchains
  - Blockchain interoperability -- how two blockchain networks talk to each other
  - Security of Blockchain-based systems
  - Use case: Decentralized Identity Management
- Hands-on:
  - Permissionless: Ethereum, Permissioned: Hyperledger Fabric
  - Use case: Hyperledger Indy / Hyperledger Cacti

Class and Grading Policies

- You should attend the classes regularly; clear your doubts during the class hours: 5% marks on attendance
- Mid Semester Examination: 25%
- End Semester Examination: 35%
- Assignments: 35% (4 assignments will be given, no extension in deadlines)
- **Assignment Groups:**
  - Create a group of two and submit through the following form **by August 4, 2024**
  - https://forms.gle/rDTdWGfCACkkwfTVA
- **Policies on Plagiarism:**
  - You are free to discuss with the instructor, TAs and your fellow classmates; however, the code should be on your own.
  - We'll use plagiarism check software, and any similarity beyond 80% will be penalized

Policy on the Use of AI Softwares like ChatGPT

- You can use AI software like ChatGPT for learning concepts, understanding a piece of code, or specific modules of the blockchain implementation platforms.
- However, the assignments should be solved by yourselves, and you should not generate the code directly from ChatGPT
- It is expected that you should be able to demonstrate the solution by executing it over a standard Linux machine with all the environments set up a priori.
  - You'll be **awarded zero marks if you cannot demonstrate** the solution or **cannot explain a part of it**, irrespective of whether the submission is correct or not.

Teaching Assistants



- Utkalika Satapathy (utkalika.satapathy01@gmail.com)
- B Shashank Goud (shashankgoud001@gmail.com)
- Sarthak Nikumbh (sarthaksham@gmail.com)

The Final Notes for Today ...

- We are not going to teach you how to do crypto trading ...
- Indeed, bitcoins and other cryptocurrencies are not the only applications of blockchain; however, they are possibly the most successful applications as of now
  - We are also not going to discuss the debate on whether cryptos are legal or not
- We'll certainly use Bitcoin as the example to discuss many of the concepts
- One important aspect of this course would be to start thinking,
  - What can be other possible stellar applications of Blockchains beyond cryptocurrencies?
  - Why those applications are not successful as of now?
  - Why should we do to make those applications successful and practically deployable?