

# CS 731: Blockchain Technology And Applications

Sandeep K. Shukla  
IIT Kanpur

C3I Center



# Acknowledgement

---

- Much material in this course owe their ideas and existence to
  - Prof. Maurice Herlihy, Brown University
  - Prof. Hagit Attiya, Hebrew University
  - Prof. Arvind Narayanan, Princeton University
  - Prof. Joseph Bonneau, NYU
  - Prof. Pramod Subramanyan, IITK

# What is Blockchain?

---

- A Linked List
  - Replicated
  - Distributed
  - Consistency maintained by Consensus
  - Cryptographically linked
  - Cryptographically assured integrity of data
- Used as
  - Immutable Ledger of events, transactions or time stamped data
  - Tamper resistant log
  - Platform to Create and Transact in Cryptocurrency
  - log of events/transactions unrelated to currency

# Why a course on Blockchain?

---

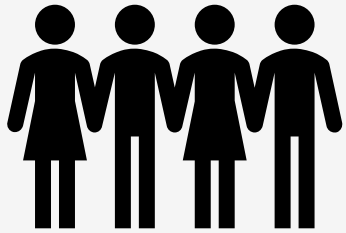
- Have you seen the news lately?
  - Bitcoin
  - Ethereum
  - Blockchain for E-governance
  - Blockchain for supply chain management
  - Blockchain for energy management .....
  - Soon: **Block chain for Nirvana**
- Is it just a hype and hyperbole?
  - Hopefully this course will teach you otherwise
  - Even if you do not care about cryptocurrency and its market volatility

# Let's First talk about Banking (a la Arvind Narayanan)

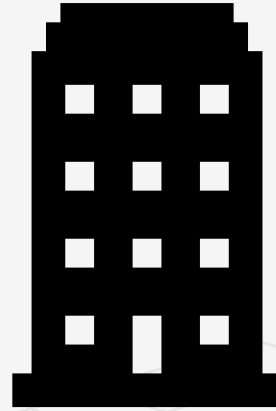
---



Regulatory Agency (RBI)



Customers



Bank



Bank Employee

# How do you transact?

---

- You write a check or do internet transaction to pay a payee
- Bank checks if you have  $\text{balance} > \text{transaction\_amount}$ 
  - If yes, it debits your account by  $\text{balance} = \text{balance} - \text{transaction\_amount}$ 
    - credit's payee's account by  $\text{payee.balance} = \text{payee.balance} + \text{transaction\_amount}$
  - If no, the transaction is invalid and rejected.
- You can check your transaction list online, or check the monthly statement
- Who maintains the ledger?
  - Bank Does
  - What if Bank allows an invalid transaction go through
    - Invalid = you did not authenticate the transaction
    - Invalid = your balance was not sufficient but transaction was made

# Bank Frauds

---

- You find a check was used to pay someone but you never wrote the check
  - Someone forged your check and/or signature
- You did sign a check for x amount, but the amount field was modified
  - How do you prove to the bank that an extra 0 was not there in your signing time?
- The monthly statement says that you did a transaction but you did not recall or the amount of a transaction is different from what you had done
  - Someone got your password, and possibly redirected OTP to another SIM (SIM Fraud)
  - Bank employees themselves might have done something
- How do you argue to the bank? (Non-repudiation)
- How do you argue that the amount was modified? (Integrity)
- Finally, do you tally your transactions when you receive your monthly statement?
  - Most people do not

# Supply chain and provenance

---

- Your buy ice cream for your restaurant from supplier B
- Supplier B actually transports ice cream made in Company C's factory
- Upon delivery, you have been finding that your ice cream is already melted
- Who is responsible?
  - Supplier B is keeping it too long on the delivery truck?
  - Supplier B's storage facility has a temperature problem?
  - Supplier C says it's supplier B's fault as when picked up – ice cream was frozen
  - Supplier B says that when received, the temperature was too high, so C must have stored it or made it wrong
  - How do you find the truth?
    - Put temperature sensors in B's truck and storage, C's factory and storage, and sensor data is digitally signed by the entity where the sensor is placed and put in a log
    - You check the log – but B and C both have hacked the log and deleted some entries?
  - What to do?



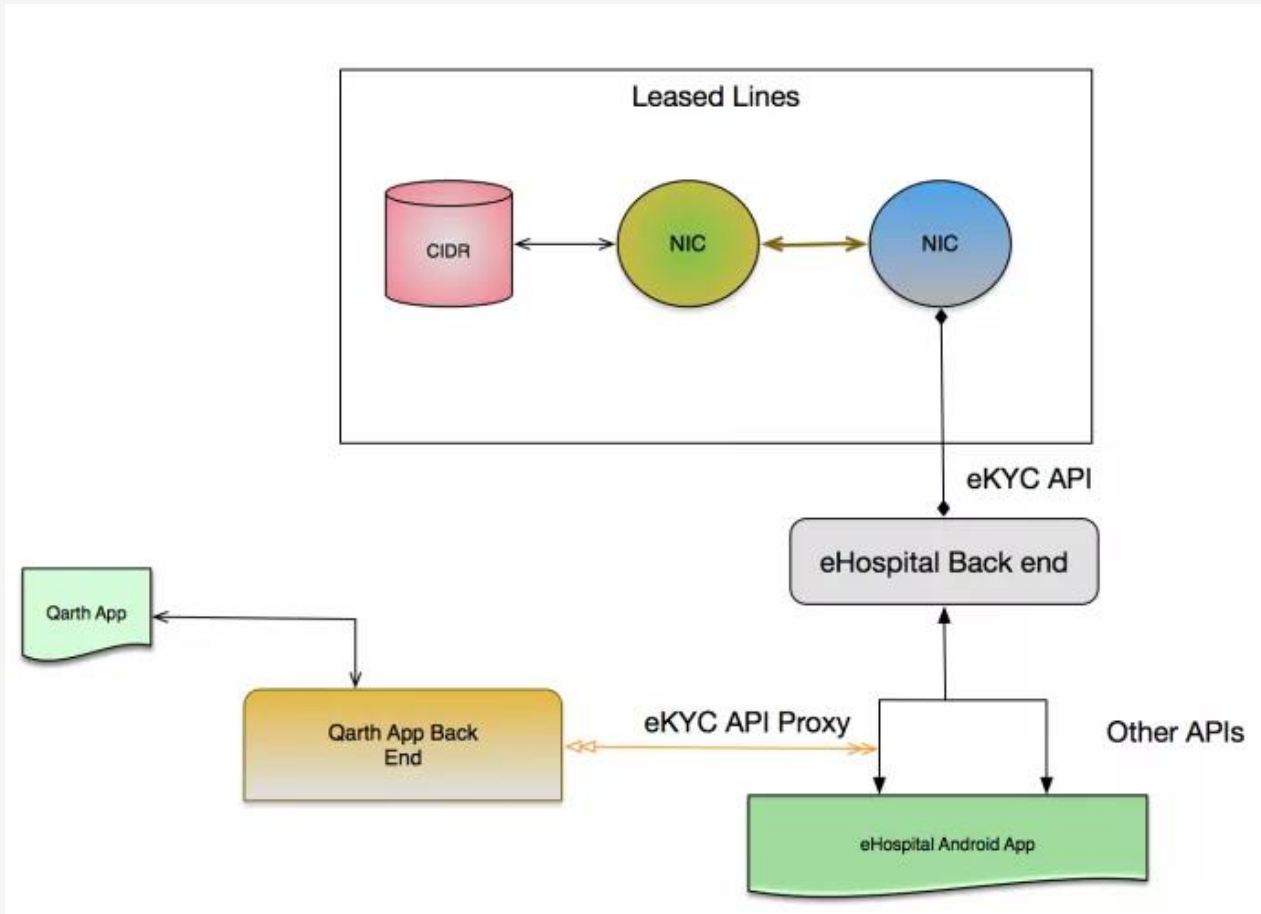
# Land Record

---

- Have you watched “Khosla ka Ghosla”?
  - You buy a piece of land
  - Someone else claims to own the land
  - But the one who sold you the land showed you paper work
  - Land registry office earlier said that the owner was rightful
  - Now they say that they made a mistake – it was owned by the other person
  - You already paid for the land – to the first person
  - First person goes missing
- How does any one prove who changed the land record?
- The government employees?

# Then there is Aadhaar

---



- E-KYC Logs
- Shown to you by UIDAI
- How do you know they did not delete important log events?
- Do you Trust UIDAI?
  - I don't

# Finally OARS

---

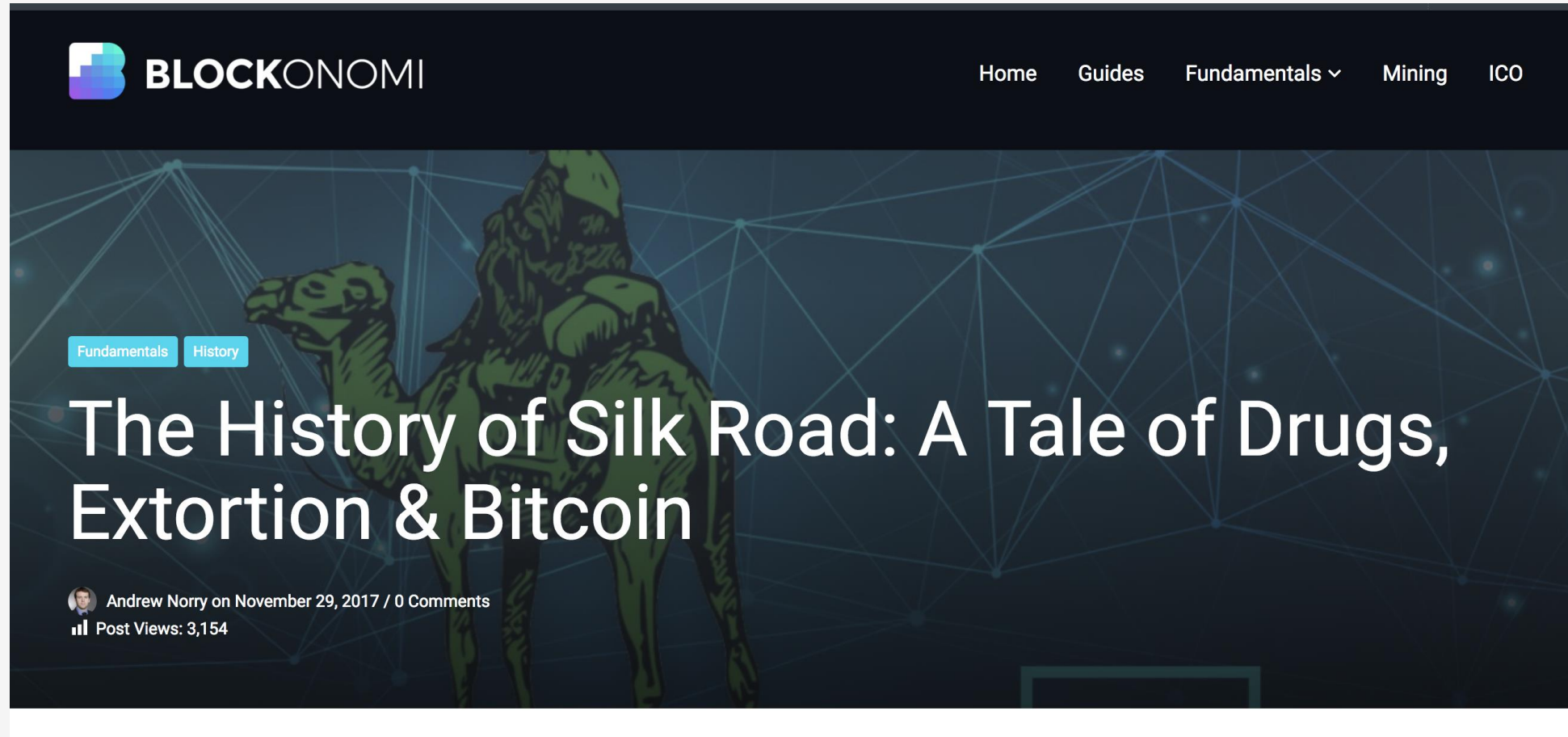


Professor	Course	Grade
1	ESC101	D
2	CS698	D
3	CS425	D
4	CS771	D



# This course is not about bitcoin or currency: Why?

---



# Why not bitcoin? (2)

---

[HOME](#) [ABOUT OUR BLOG](#) | [BLOCKONOMICS WEBSITE](#) [Q](#)



Frederick Coleman [Follow](#)

Manager Media and Communications— Blockonomics

Jun 16, 2017 · 6 min read

## The Dark Side of Bitcoin: Illegal Activities, Fraud, and Bitcoin



# Why not bitcoin? (3)



# Why not bitcoin? (4)

---

BLOCKCHAIN VC TOP 10 STORIES | SXSW HACKATHON 🔍

## Proof of work, or proof of waste?

### Bitcoin and the energy usage dilemma

If you're moderately well versed in the blockchain ecosystem, then you would have by now come across the energy consumption debate that is taking place in relation to Bitcoin Mining. Yes, Bitcoin Mining requires a lot of energy, and not a modest amount either. Mining (under the current protocol of Bitcoin's *proof of work* algorithm) is **deliberately** consumptive of energy.



# Why not bitcoin? (5)

---

## Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa

f 21.9k in 0 g+ Share t Tweet





# Why not bitcoin? (6)

tainment Tomorrow Video Reviews Events US Edition

Entirely predictable...  
so you don't have to be. | mapquest | Get the app


AdChoices

---

## China reportedly wants to curtail wasteful bitcoin mining

It doesn't like the waste and fears a crash would cause economic havoc.

---

 Steve Dent, @stevetdent  
01.08.18 in [Business](#)

4  
Comments

354  
Shares

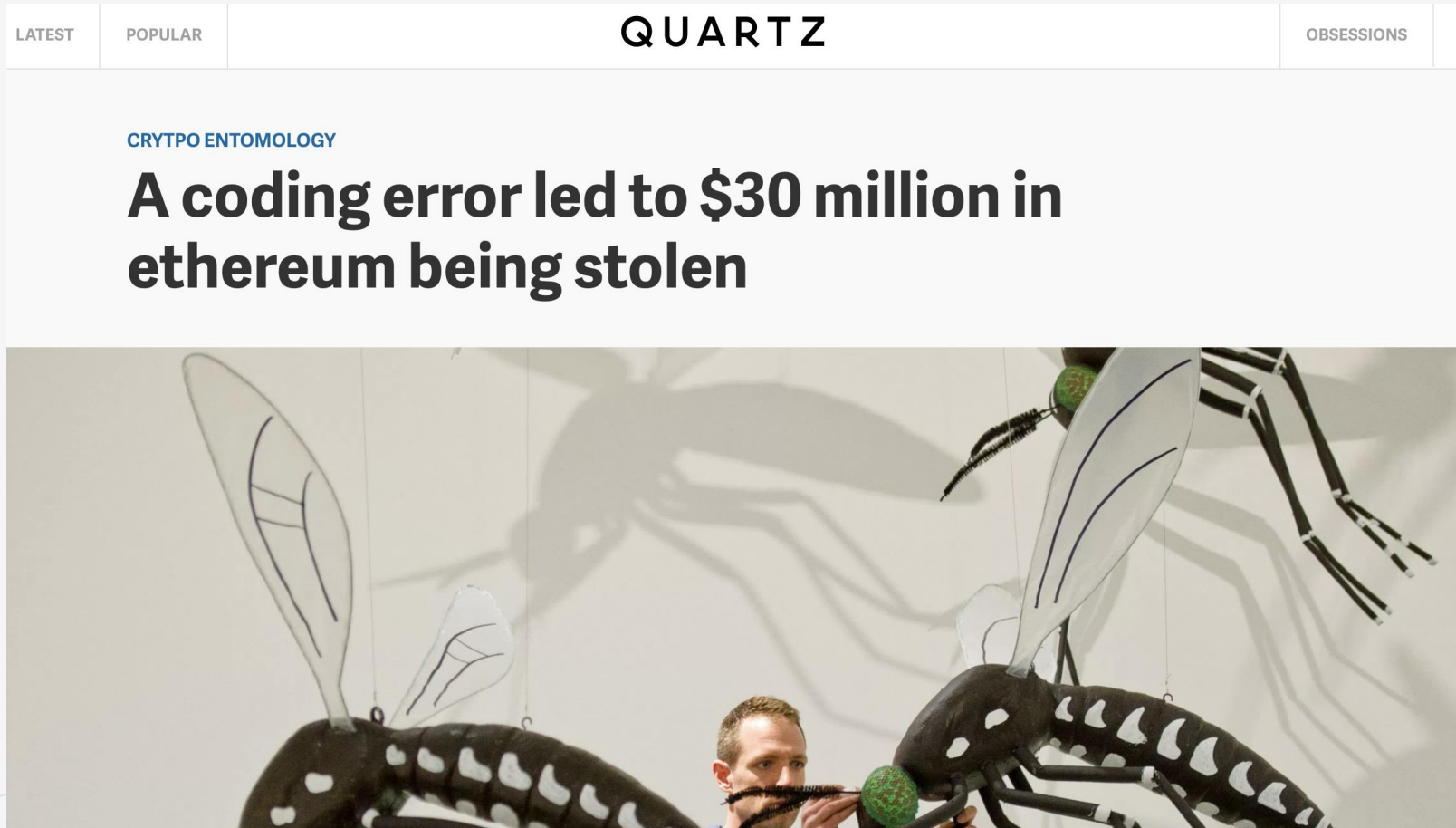
# Why no money business?

---



# Why no money business? (2)

---



# Bitcoins and other cryptocurrencies

---

- Too much interest by investors to park their assets
- Less use as a medium of value exchange
- Private Key stealing or private keys at exchanges — risk
- Coding vulnerabilities — risk
- Volatility
- Energy Waste — climate impact
- Too much concentration in one country — risk
- Regulatory risk
- Usage for criminal activities — Silk Road

# Again, What is a blockchain?

---

- Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activities and therefore cybersecurity concerns as a whole.
- Attractive properties of Blockchain
  - Log of data with digital signature
  - Immutable (once written - cryptographically hard to remove from the log)
  - Cryptographically secure - privacy preserving
  - Provides a basis for trusted computing on top of which applications can be built

# Trust Model

---

- Cyber Security is all about who you trust?
  - Trust your hardware to not leak your cryptographic keys?
  - Trust your O/S to not peek into your computation memory?
  - Trust your hypervisor to not mess up your process memory?
  - Trust your application to not be control hijacked or attack other applications?
- Where is your trust anchor?
  - Hardware?
  - Operating system?
  - Application?
  - Manufacturer?

# Trust Model (2)

---

- In many real life transactional activities – trust model is the inverse of the threat model
  - Do you trust your bank to not take out small amounts from your balance all the time? (Watch – “Office Space”)
  - Do you trust the department of land records to keep your record’s integrity?
  - Do you trust UIDAI officials to keep your aadhaar data from unauthorized access?
  - Do you trust your local system admins to not go around your back and change settings, leak passwords, change database entries, and remove their action from system logs?
  - In the patch management system of your enterprise, are the patches being put -- all have digital certificates? Who put them? Do you trust your employees to do the correct thing and not put a malware as patch?

# Back to Banking Example (Arvind Narayanan)



# Arvind Narayanan's Goofycoin

---



GoofyCoin

Goofy can create new coins

signed by  $pk_{\text{Goofy}}$

CreateCoin [uniqueCoinID]

New coins belong to me.



A coin's owner can spend it.

signed by $pk_{\text{Goofy}}$
Pay to $pk_{\text{Alice}}$ : $H( )$

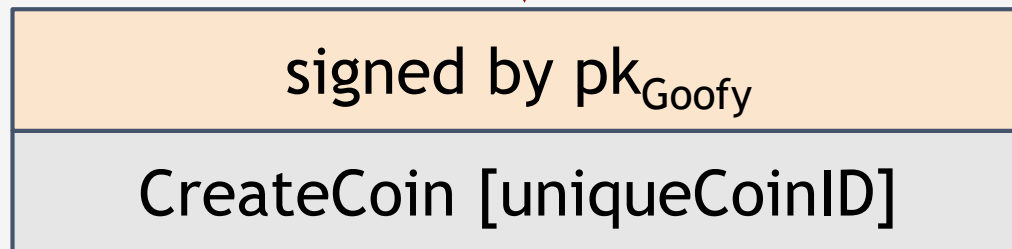
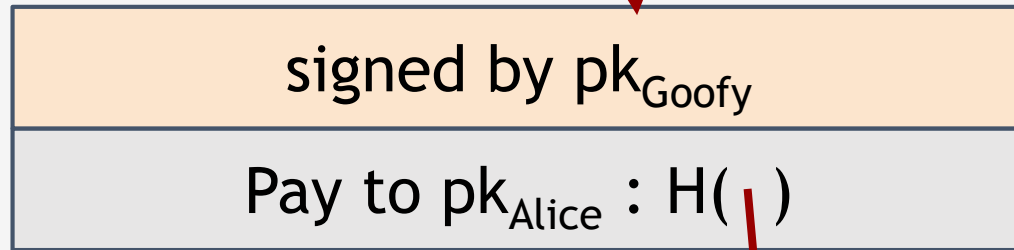
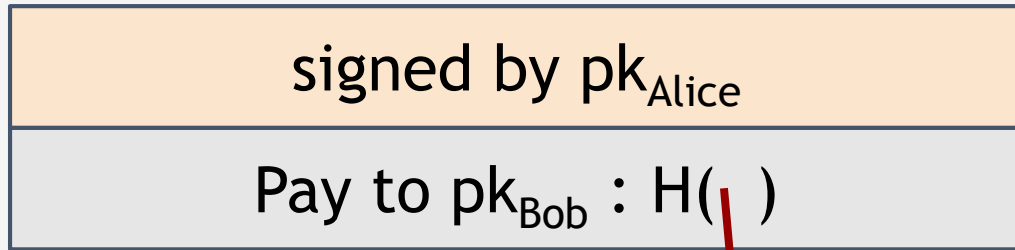


signed by $pk_{\text{Goofy}}$
CreateCoin [uniqueCoinID]

Alice owns it now.



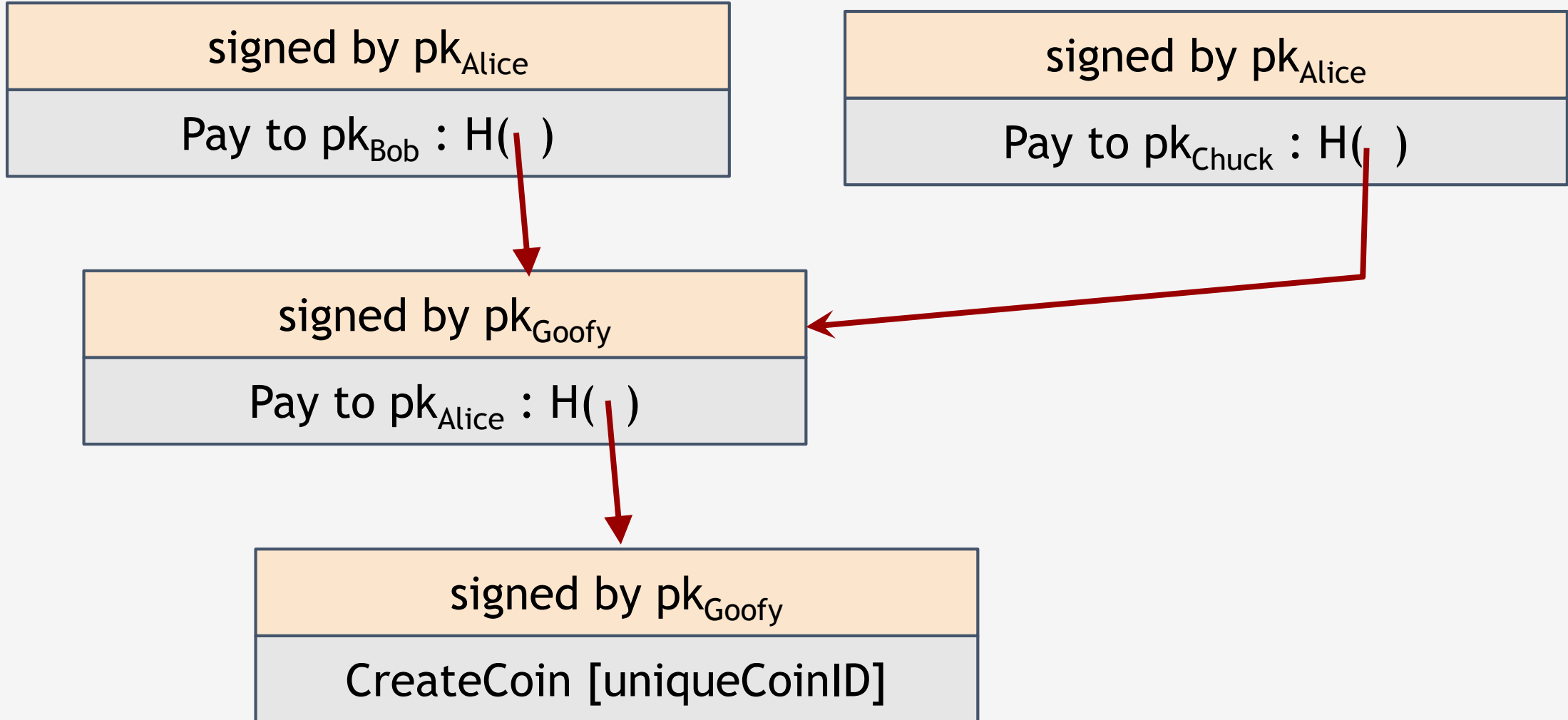
The recipient can pass on the coin again.



Bob owns it now.



# double-spending attack



# double-spending attack

---

the main design challenge in digital currency

## Arvind Narayanan's ScroogeCoin – Double Spending Proof Digital Currency

---

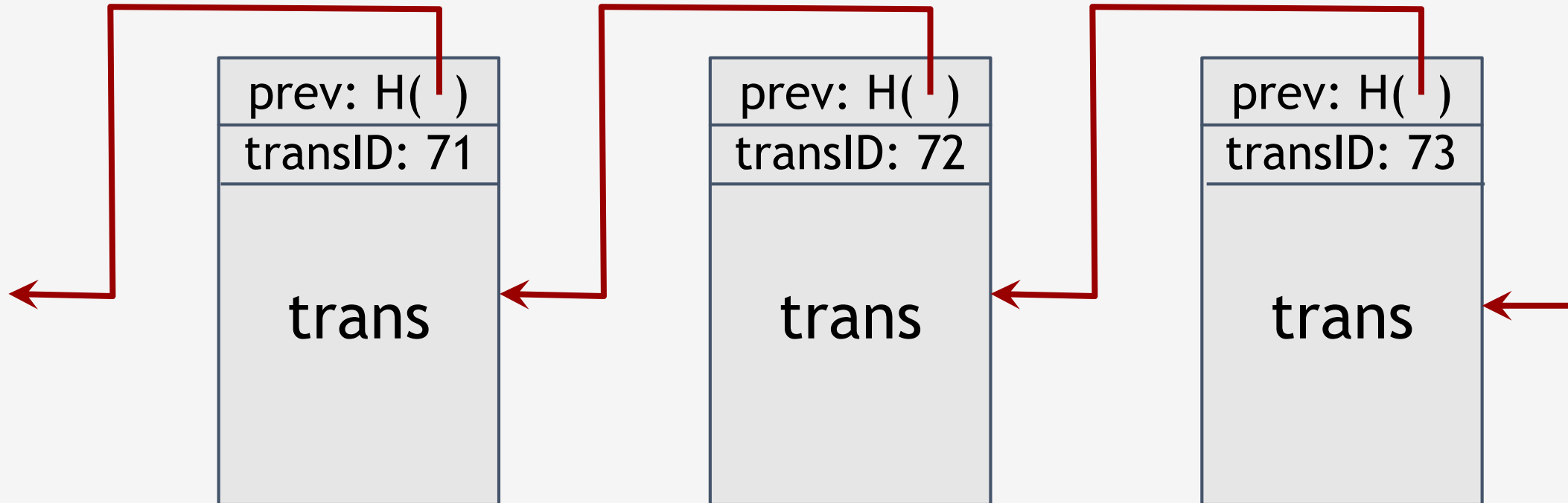


ScroogeCoin

Scrooge publishes a history of all transactions  
(a block chain, signed by Scrooge)



$H( )$



optimization: put multiple transactions in the same block



## CreateCoins transaction creates new coins

Valid, because I said so.

transID: 73    type:CreateCoins		
coins created		
<i>num</i>	<i>value</i>	<i>recipient</i>
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...

← coinID 73(0)

← coinID 73(1)

← coinID 73(2)



PayCoins transaction consumes (and destroys) some coins,  
and creates new coins of the same total value

consumed coinIDs: 68(1), 42(0), 72(3)		
coins created		
<i>num</i>	<i>value</i>	<i>recipient</i>
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...
signatures		

Valid if:

- consumed coins valid,
- not already consumed,
- total value out = total value in, and
- signed by owners of all consumed coins

## Immutable coins

---

Coins can't be transferred, subdivided, or combined.

But: you can get the same effect by using transactions  
to subdivide: create new trans  
consume your coin  
pay out two new coins to yourself

Don't worry, I'm honest.

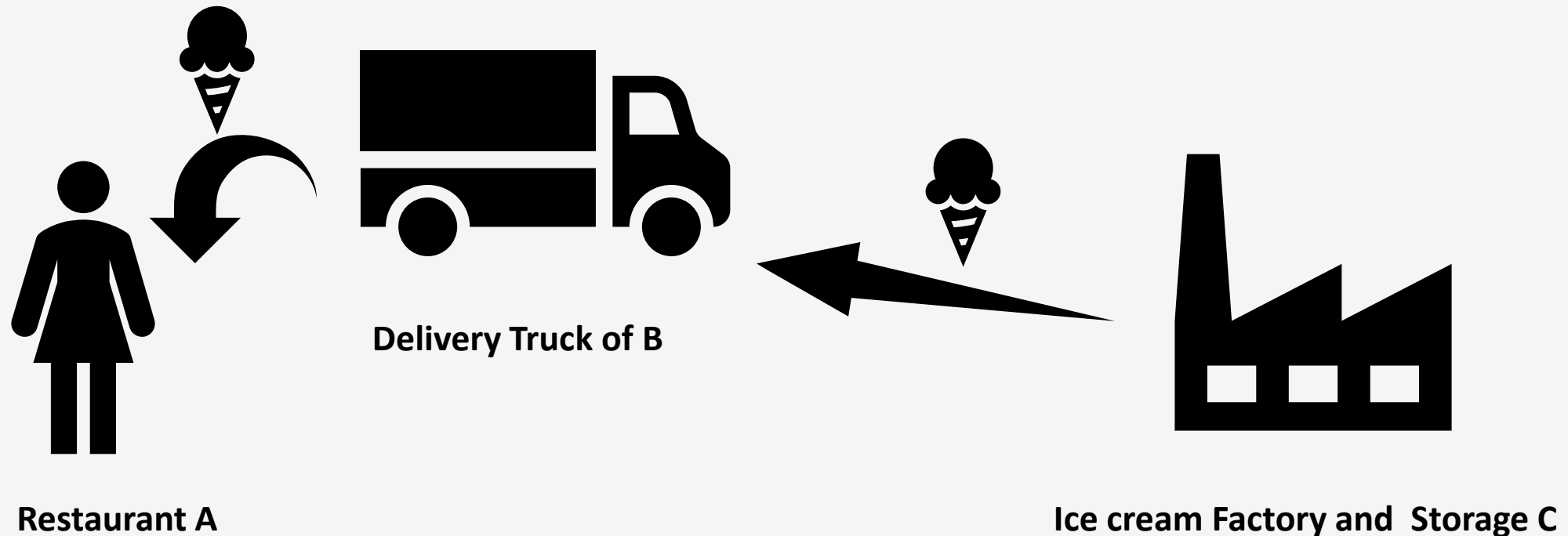


Crucial question:

Can we descroogify the currency,  
and operate without any central,  
trusted party?

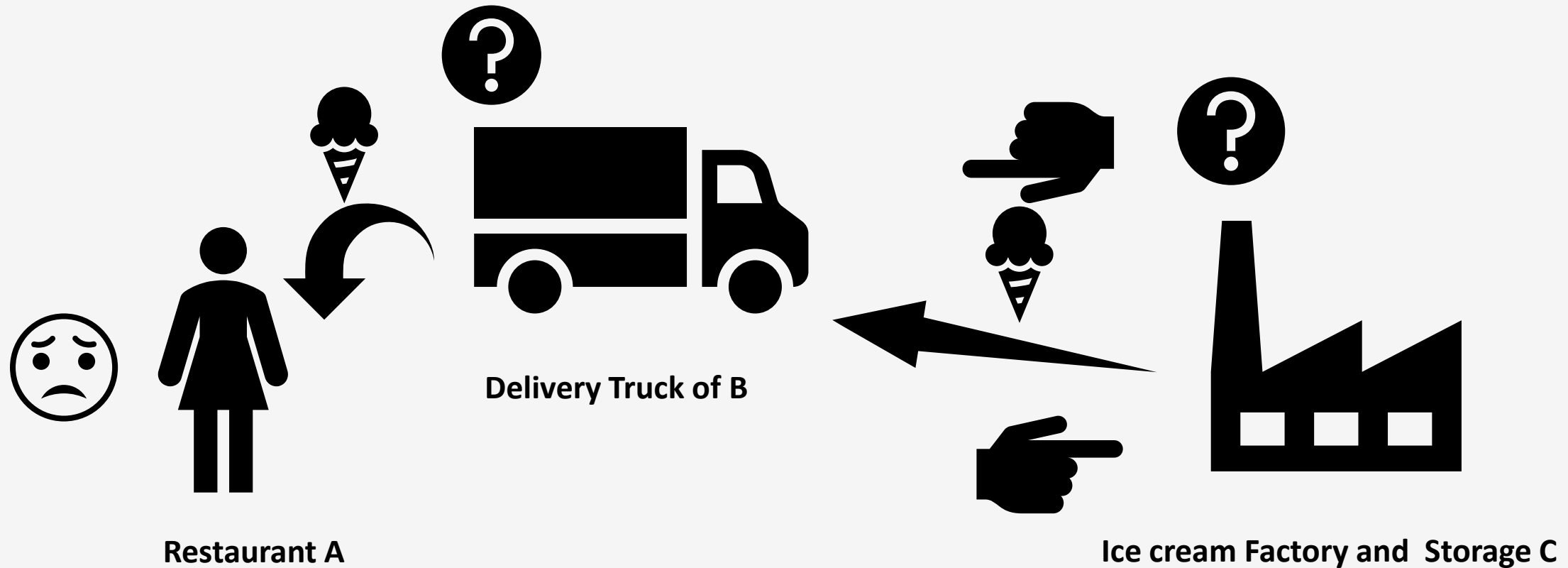
# Back to the supply Chain Story (Herlihy)

---



**Ice Cream Supply Chain to Restaurant A from Factory C via Supplier B**

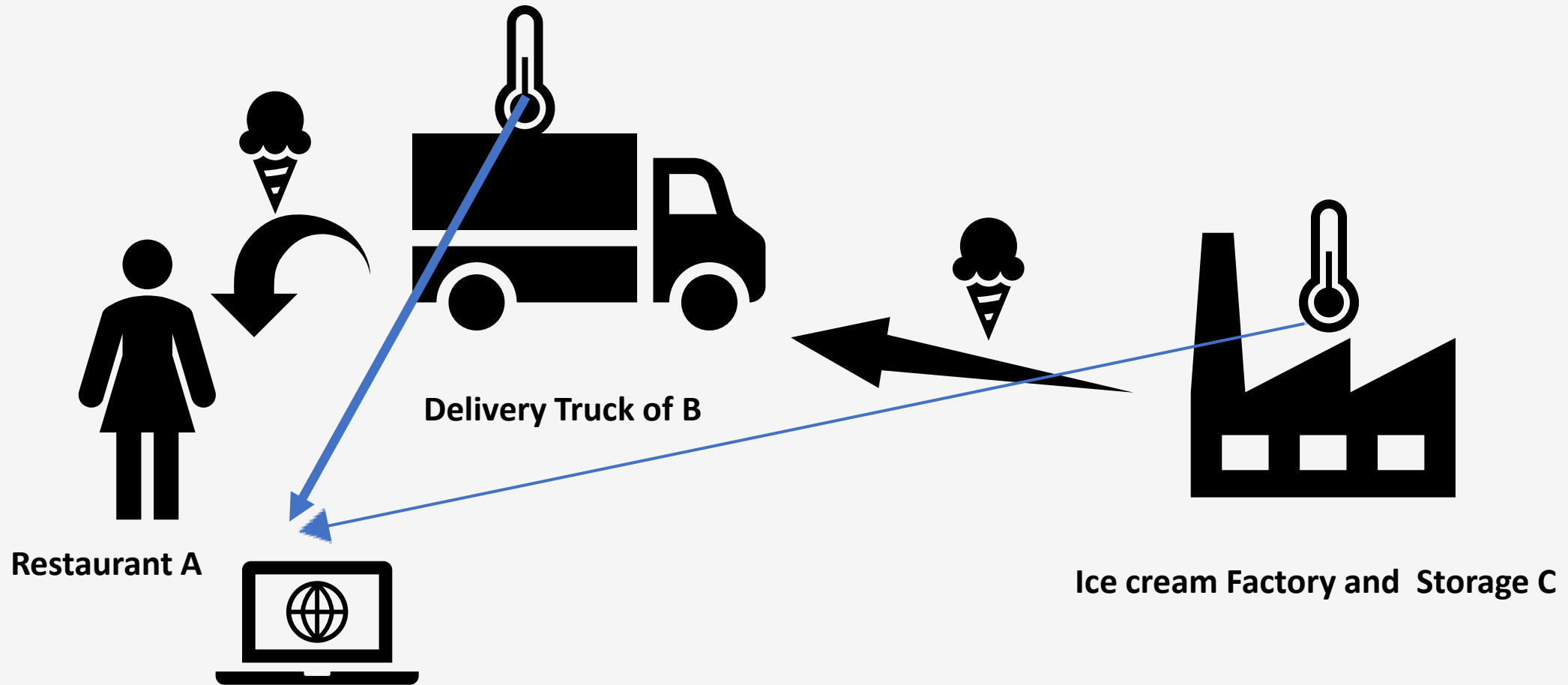
# Ice cream is melted



**Ice Cream Supply Chain to Restaurant A from Factory C via Supplier B**

# Use IoT to create non-repudiation

---



**IoT sensors send real-time data to the server at Restaurant A to periodically show the factory and the truck temperatures to Restaurant A**

# What can go wrong?

---

- IoT sensor data may be intercepted by a middle man and changed before it reaches the server (**data integrity**)
- IoT sensors may be stopped and old readings may be replayed (**replay attack**)
- What the server gets purportedly from factory C, may be manufactured by supplier B (**Authenticity**)
- If restaurant A claims that C's temperature reading shows that ice cream was melting in the storage, C can say that message you received is not from me – there was an MITM attack (**repudiation**)
- So restaurant A will not be able to pinpoint any one in the supply chain with full confidence!!



# What can be done?

---

- Use a message integrity proof (**Hashing**)
- Use digital signature of the individual IoT devices (**Authenticity and non-repudiation**)
  - assuming the digital signatures cannot be forged
  - private keys are kept safe
- Use authentic time stamping with the IoT data before hashing for integrity (**avoid replay attacks**)
- So now factory A can pinpoint with some basic security assumptions about this infrastructure

# Concurrency Issue

---

- A has other suppliers for other goods required for its business (multiple concurrent supply chains)
- B and C has multiple other consumers of their services
- So if there are  $N$  suppliers who are also consumers of some of these entities, we have an  $N^2$  messaging problem

A offers that every one can look up their data from my server, so you can get linear number of messaging

But do you trust A as purveyors of your data?

# Solutions?

---

- Have a trusted authority or a cloud provider to become a publish-subscribe service provider
- Every supplier sends their IoT data with message integrity, authentication code etc to the cloud server
  - Every consumer subscribes to the events they are interested in on the cloud
  - Every supplier becomes authenticated data generator on the cloud

What if the cloud provider cannot be trusted?

# Create a framework on which data is crowd sourced, validated by the crowd for the crowd?

---

- You get a block chain
- But now the question is as concurrent messages come in to this framework, how do you order them?

DISTRIBUTED CONSENSUS IS REQUIRED TO DECIDE

ordered

1. of all messages coming in concurrently how are they

2. But if some of the crowd are malicious, and tries to allow data that are wrong, or ordered wrong?

3. You need Byzantine fault-tolerant consensus

# Conclusion of the First Lecture

---

- Blockchain is about

- Distributed Record Keeping
- Trust Model varies – but usually single point of trust is not good
- Based on Trust Model –
  - Permissioned Blockchain
  - Non-permissioned or public block chain
  - Also, private blockchain
- Data integrity (No one has tampered with the data after its creation)
- Authenticated Transactions or event logging
- Strong Cryptographic Application

- Blockchain is certainly not ONLY

- Cryptocurrency
- In this course, cryptocurrency will be avoided

# Summary of Lecture 1

---

- What did you learn today?

- The need to learn about block chain technology and its applications
- Bitcoin and Cryptocurrencies are only an example application of the technology
- This course is not about Bitcoin or Cryptocurrency – but more on the technology and applications
- Trust Model determines whether you need blockchain and if so – what kind – permissioned/permissionless/private
- Basic issues leading to the Bitcoin (Trust model again)
- Basic issues in supply chain provenance and integrity and trust model
- Concurrency is important to take into account
- Fault-tolerant Consensus is a requirement for handling concurrency and trust model issues