SETTING THE STAGE

Siddhesh V Naik
Anil Dongre

DISCLAIMER

The opinions presented/stated during this workshop are of the speakers alone. They are not to be attributed to anyone else.

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

AGENDA

- ✓ The Problem
- ✓ Solution Attempts
- ✓ Need For Decentralization
- ✓ Laying The Bricks

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 1 – THE CREDIT SALE

Through the month

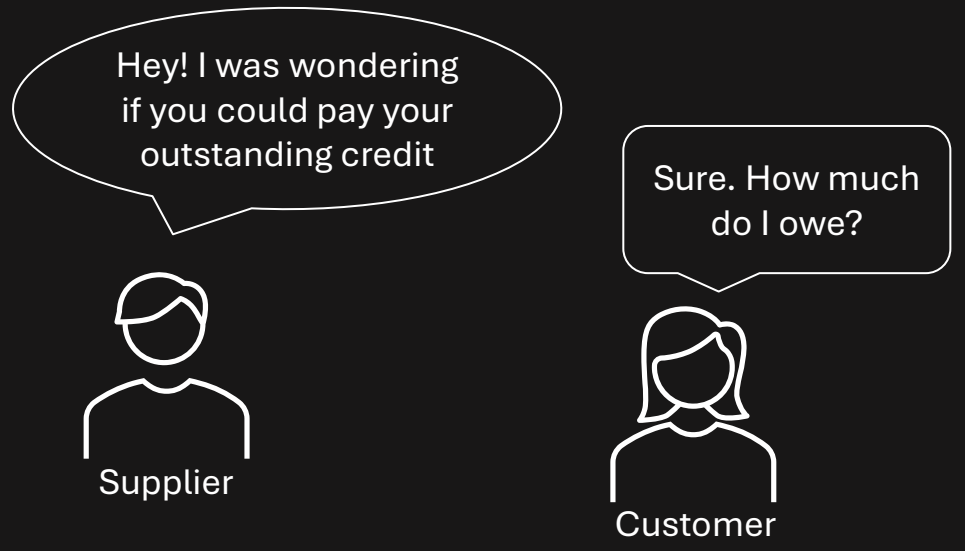
Supplier maintains the records

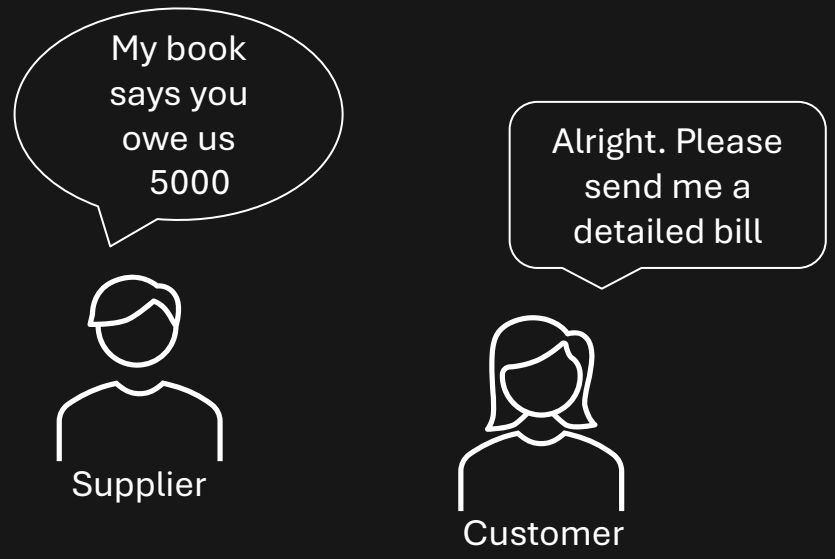
THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 1 – THE CREDIT SALE

Supplier maintains the records

31st of the month



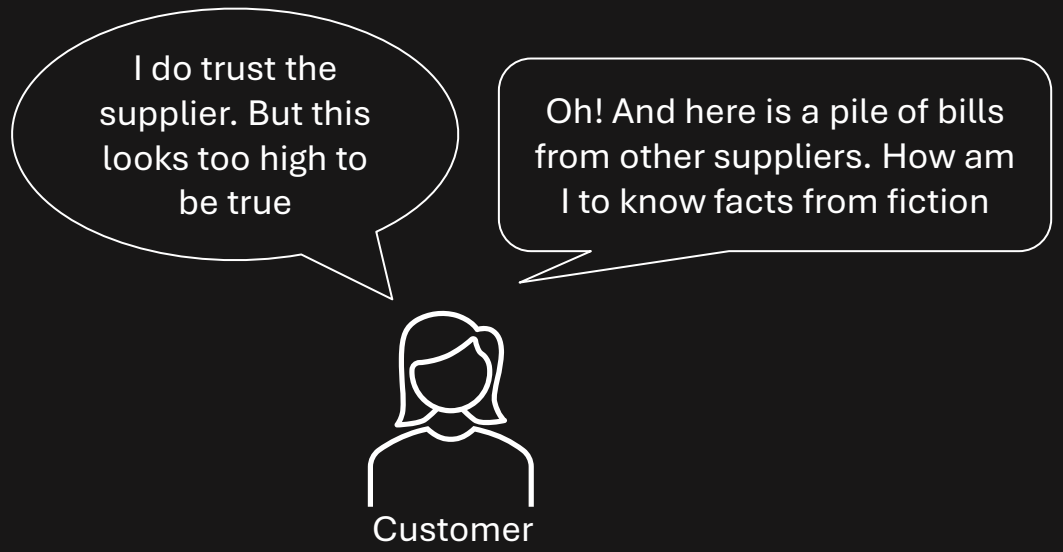


THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 1 – THE CREDIT SALE

Supplier maintains the records

On receipt of the bills

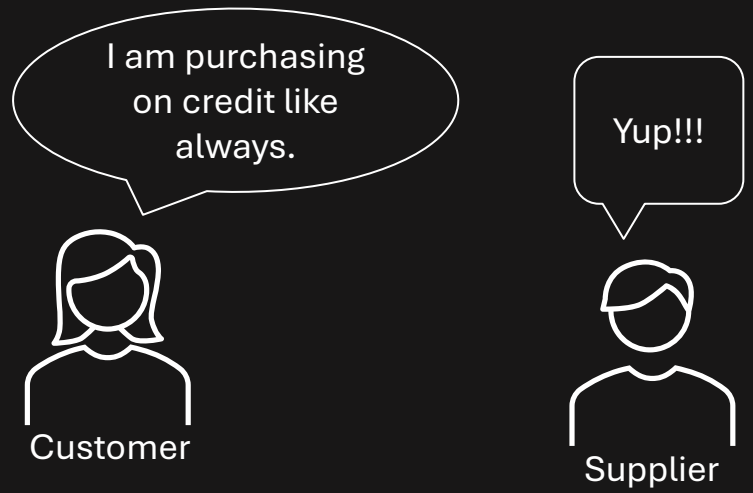


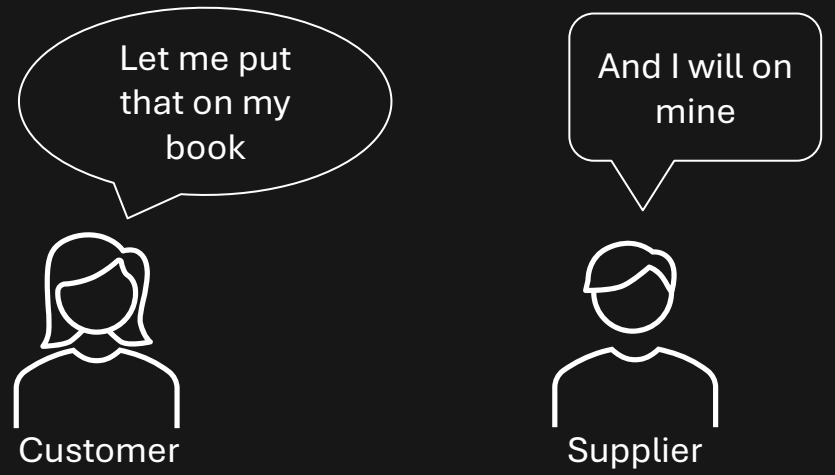
THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

How do we solve this?

SCENE 2 – THE CREDIT SALE

Through the month





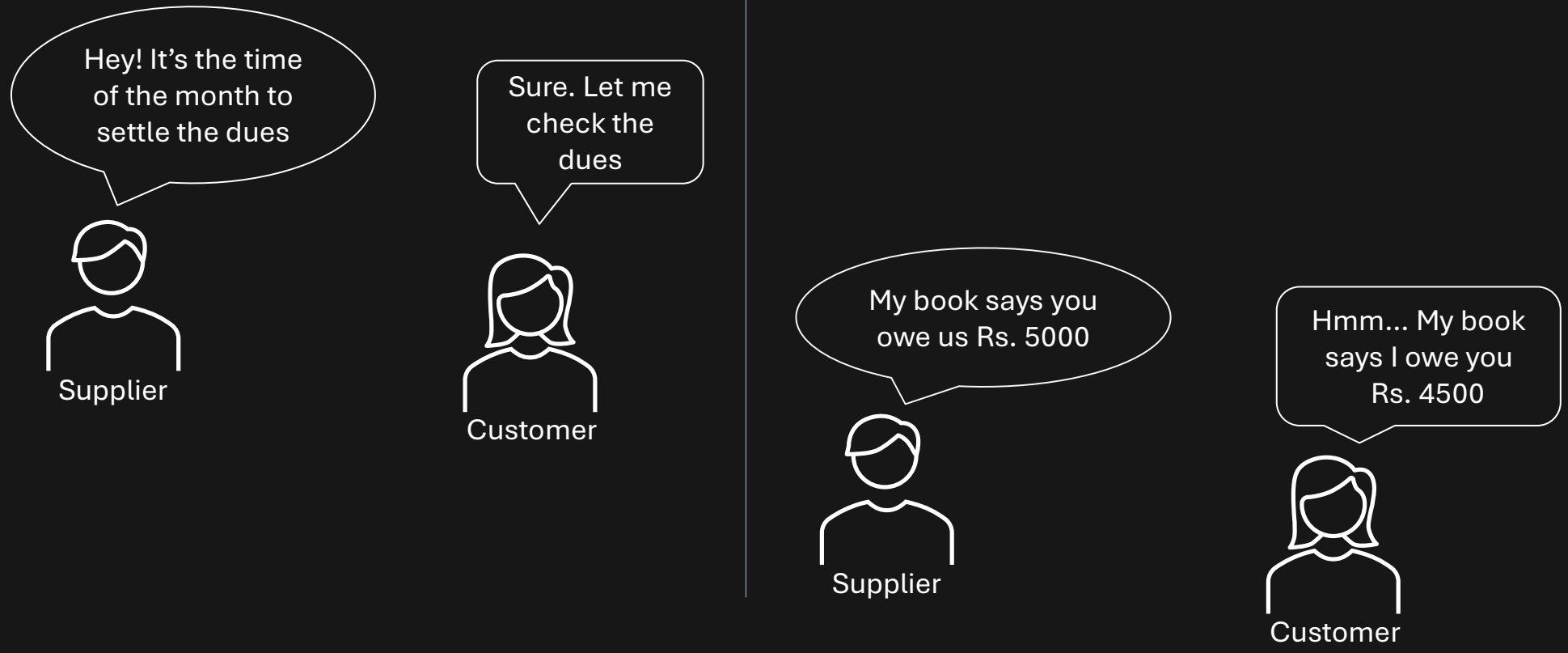
Supplier & Customer maintain their own records

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records

31st of the month

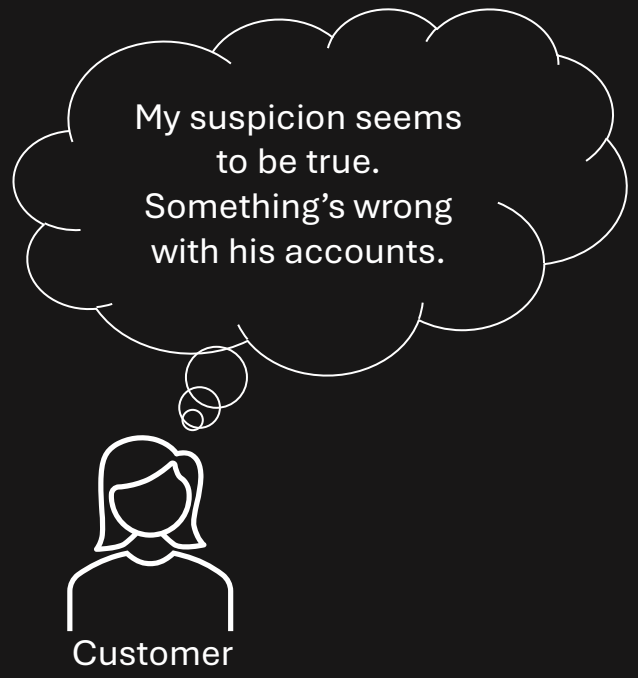


THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records

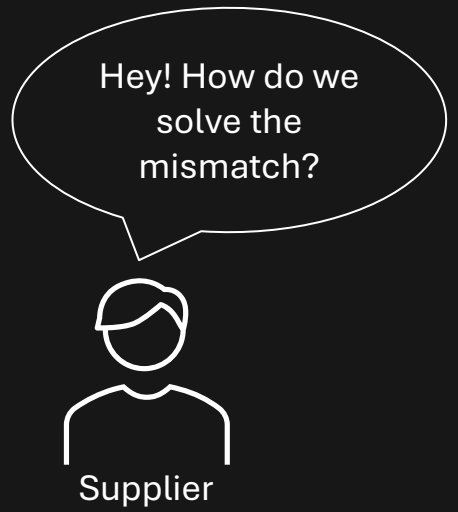
A few moments later



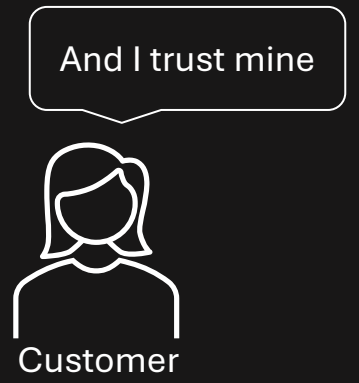
THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records



After a few days

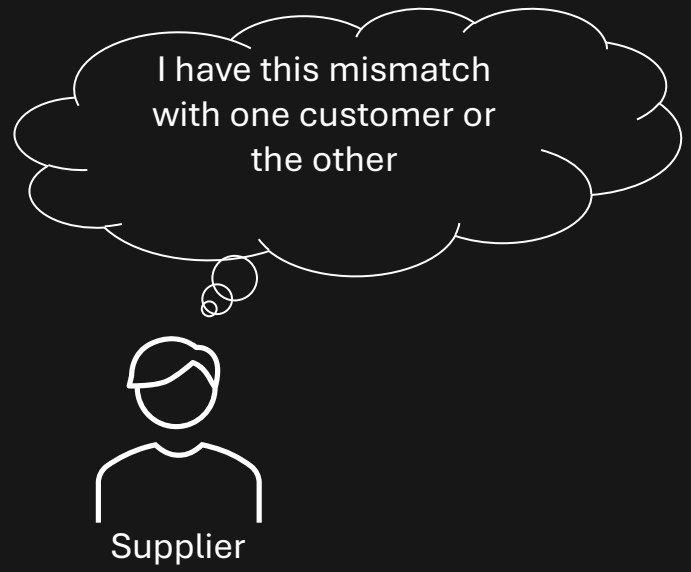


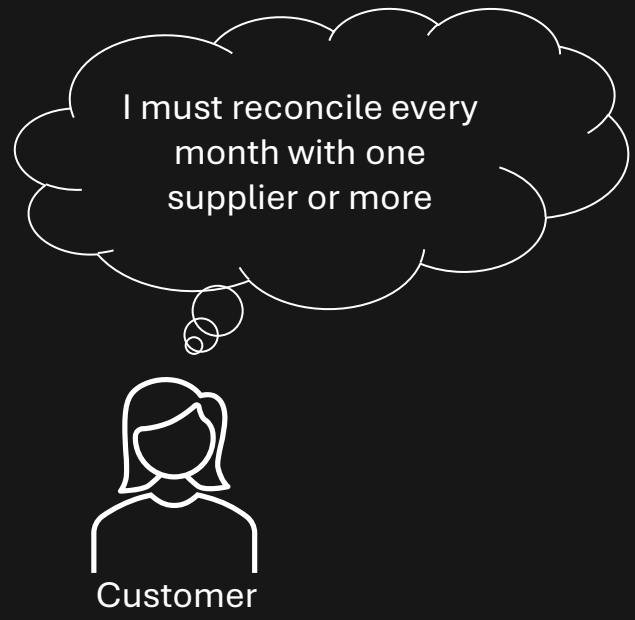
THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records

Every month

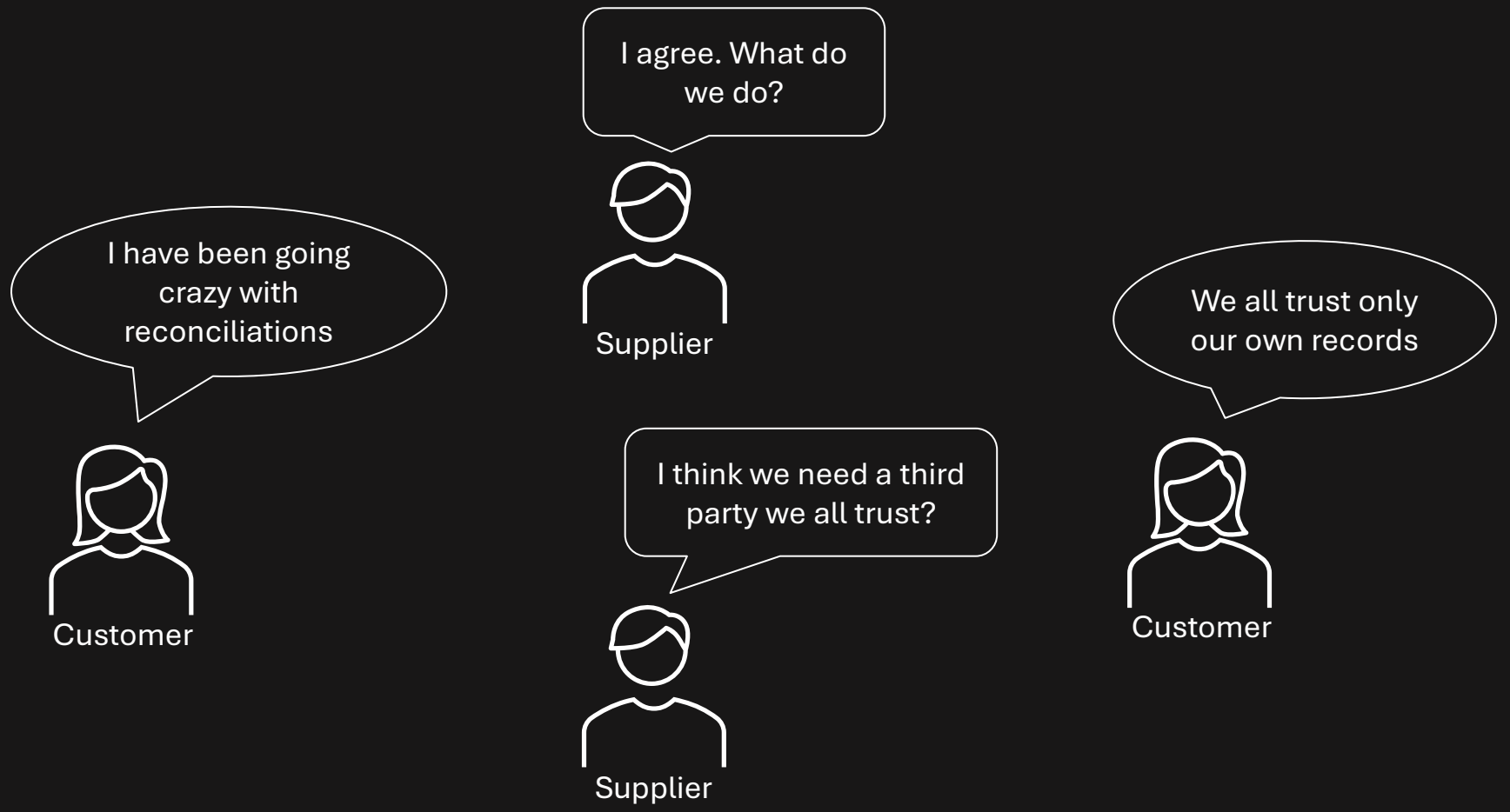




THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

How do we fix this?

SCENE 3 –SUPPLIER CUSTOMER CONF



Let's get an intermediary

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 3 –THE INTERMEDIARY

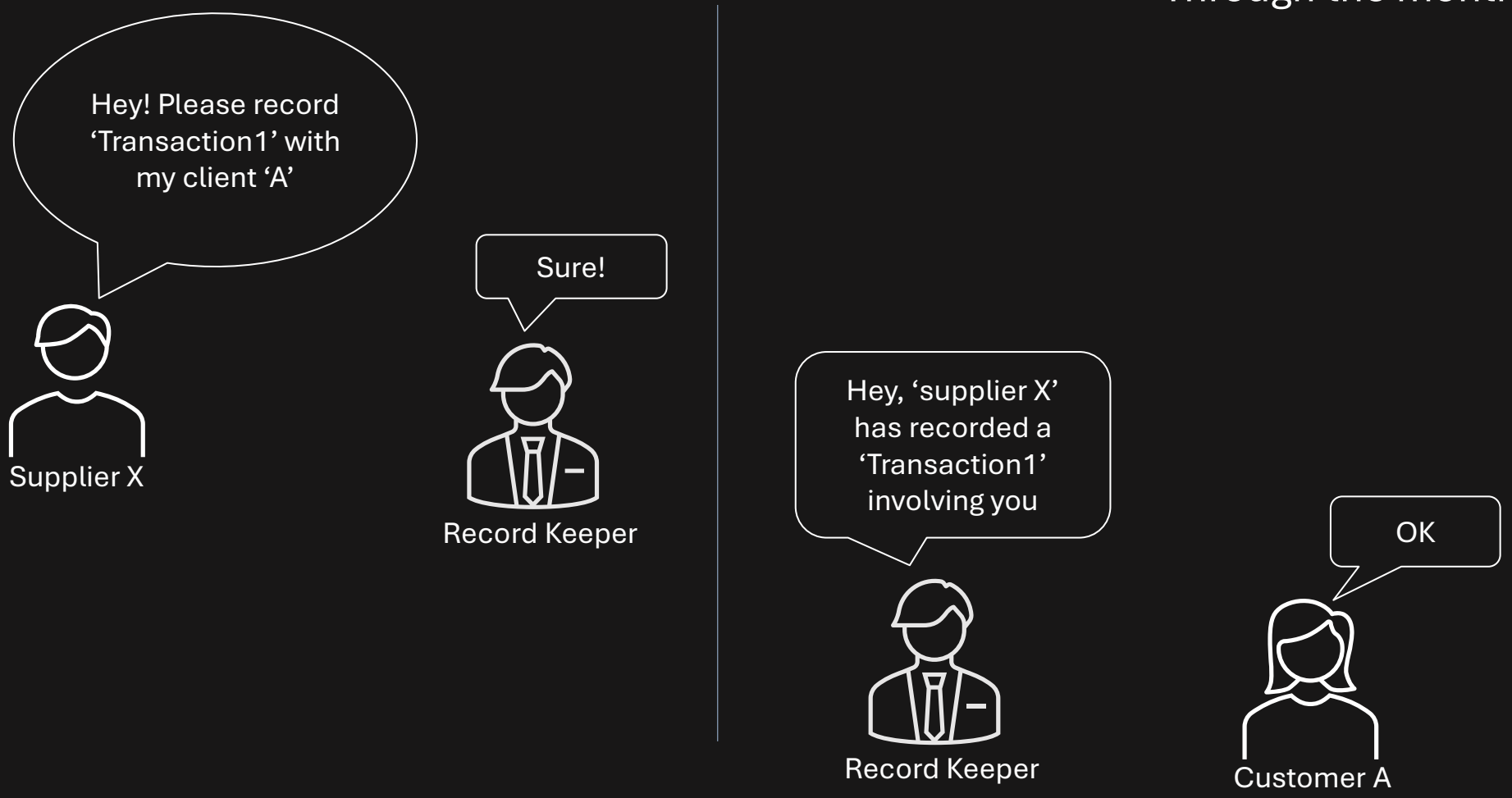
Let's meet our intermediary

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 3 – THE CREDIT SALE

Transacting with the help of intermediary

Through the month

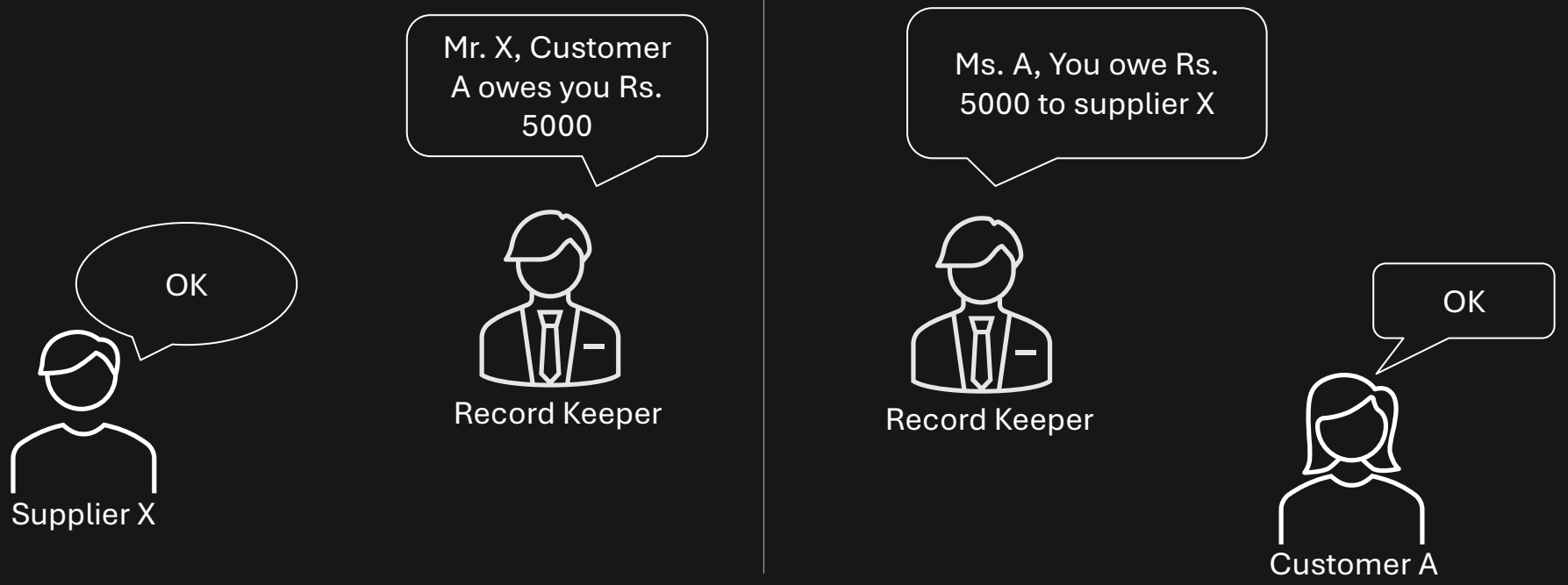


THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SCENE 3 – THE CREDIT SALE

Transacting with the help of intermediary

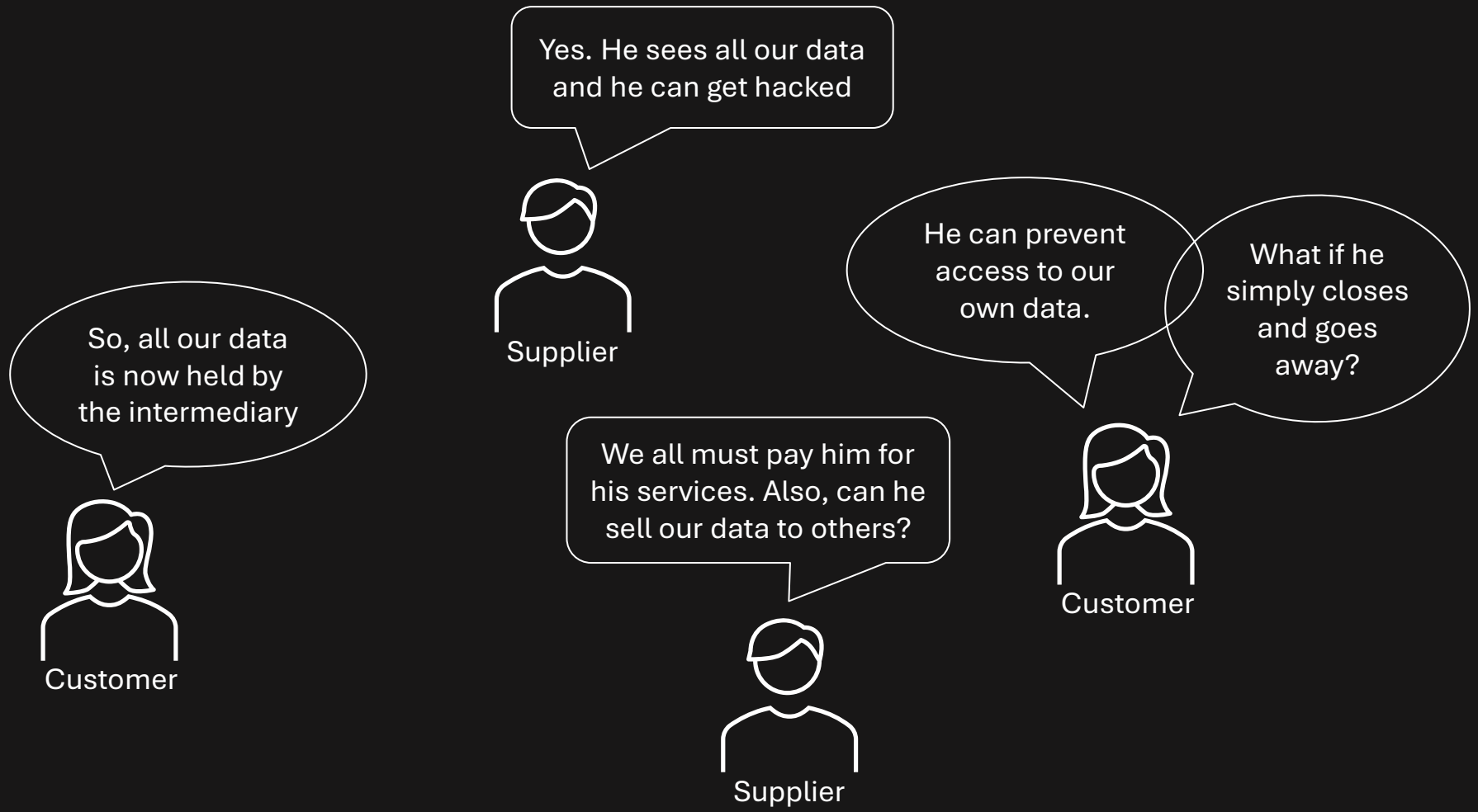
31st of the month



THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

Can you name some intermediaries?

SCENE 4 – ANNUAL MEETING



We thought a 3rd party would help. But it has its own problems

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

Can you identify problems with having an intermediary?

PROBLEMS

PRIVACY

The intermediary has complete view of the data, and further can even share it with a third party without our knowledge

CENSORSHIP

The intermediary can at any point restrict the clients from using the services or accessing their own data

SINGLE POINT OF FAILURE

Any issues in the intermediary's infrastructure renders the whole ecosystem nonfunctional

COSTS

In an asymmetrical relationship the intermediaries mostly have an undue advantage in dictating the fees

DATA SECURITY

The data collected acts as a honey pot and despite several measures, data breaches are a frequent occurrence

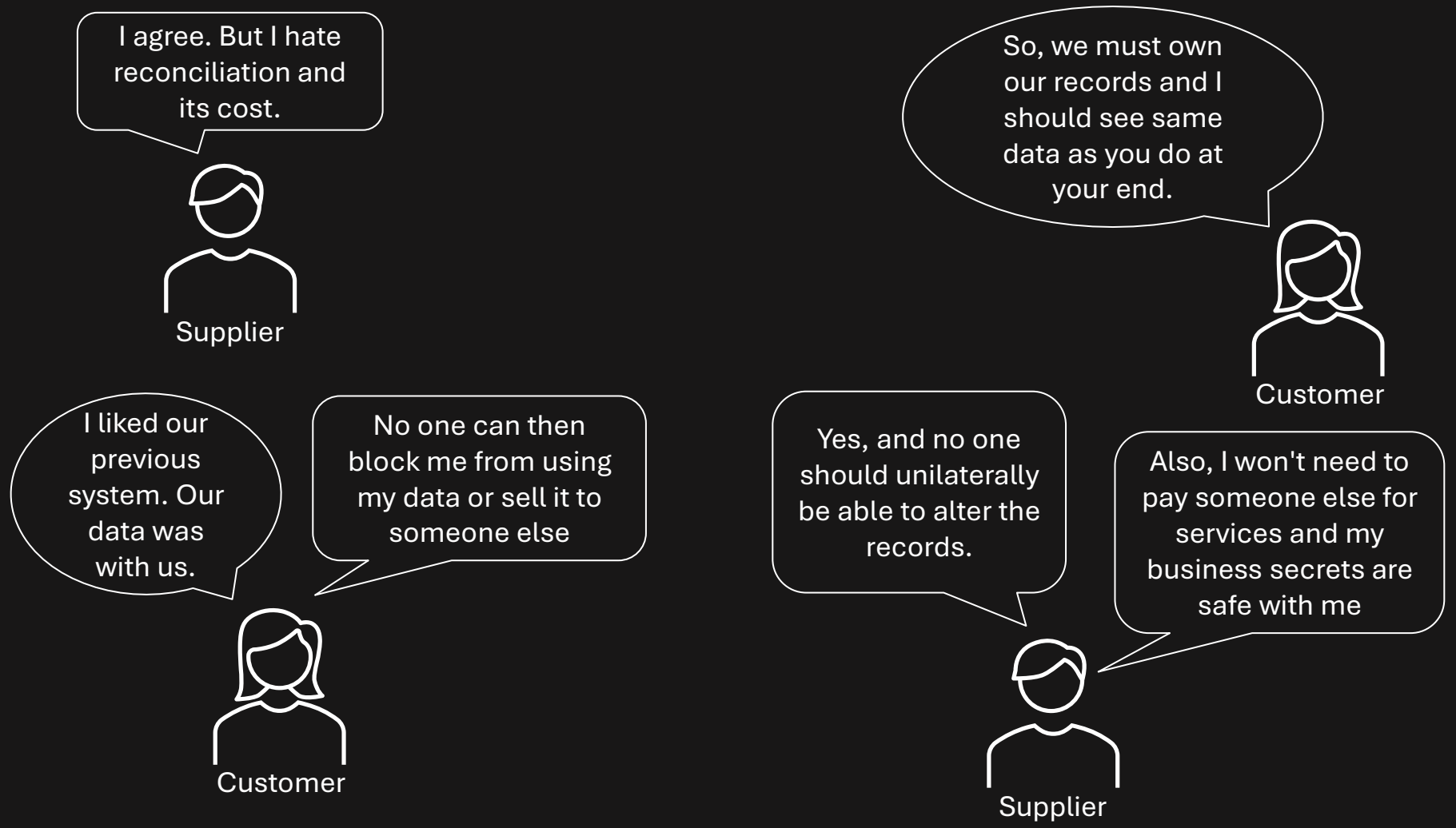
DATA TAMPERING RISK

With no second source of truth available for verification, there is no security against the intermediary unilaterally modifying the data

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

So, using an intermediary has its own problems.
What do we do now?

SCENE 4 – ANNUAL MEETING



We need our old system but a new approach

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

Wait a min, intermediaries like banks, exchanges, e-commerce portals have existed for decades and centuries. That means they have served us well for a reason. No?

WHAT KEEPS INTERMEDIARIES IN CHECK?

1. REGULATIONS

For many industries, the government sets regulations and provides oversight to ensure smooth functioning. For e.g., Regulations such as Anti Money Laundering law and entities such as RBI and SEBI for finance domain

2. COMPETITION

Multiple service providers in same space are competing for clients. Any malpractice would drive clients to competitors hampering long term gains

However, these are reactive measures. Without a solution inherent to the design a reliable system is difficult to achieve

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

Now that we mentioned banks let’s try to imagine what will it take to eliminate banks?

Let’s build one brick at a time

Its time we meet a team of engineers who are trying to solve the same problem.

MEETING WITH ENGINEERING TEAM

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

WHAT IS MONEY?

- Money is a global database to track ‘I Owe You’
- The amount of money you have is a marker for how much the world owes you
- Currency is a form of money

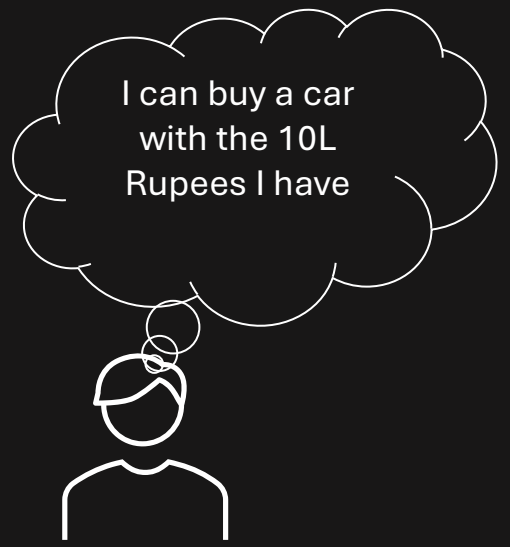
COMMON FORMS OF CURRENCY

- Cash
- Records in banks ledger

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

FUNCTIONS OF CURRENCY -1

Store of Value

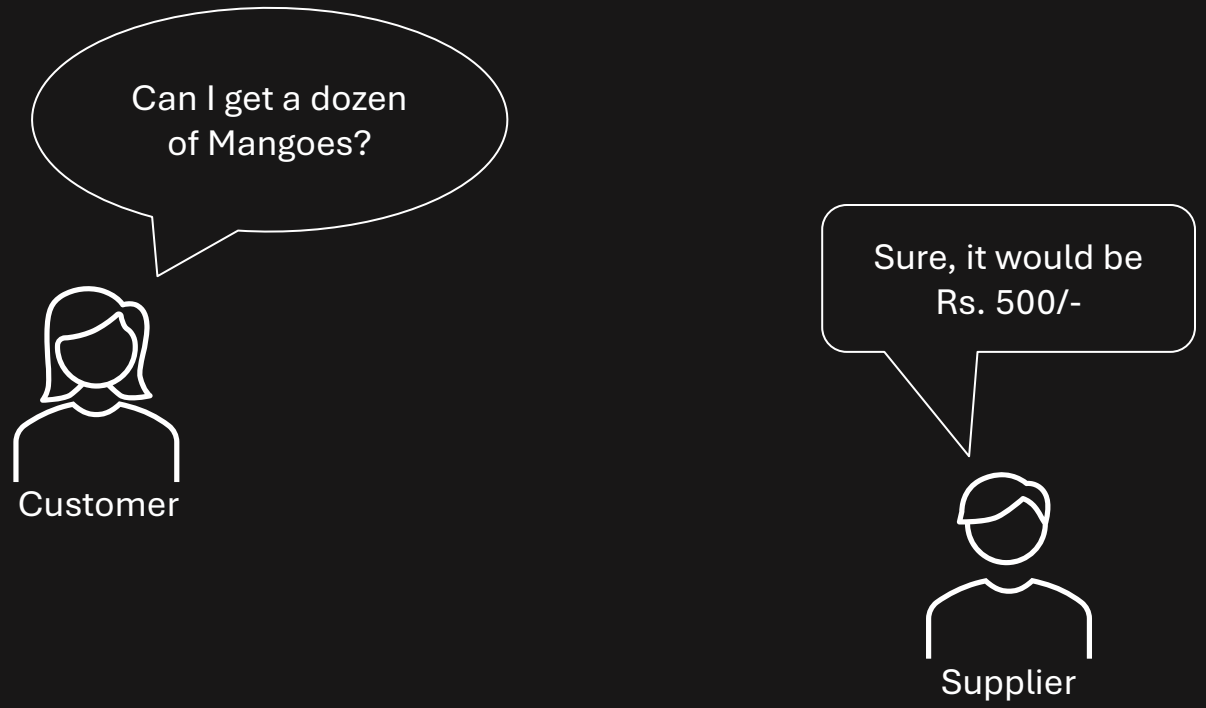


After 3 years

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

FUNCTIONS OF CURRENCY 2

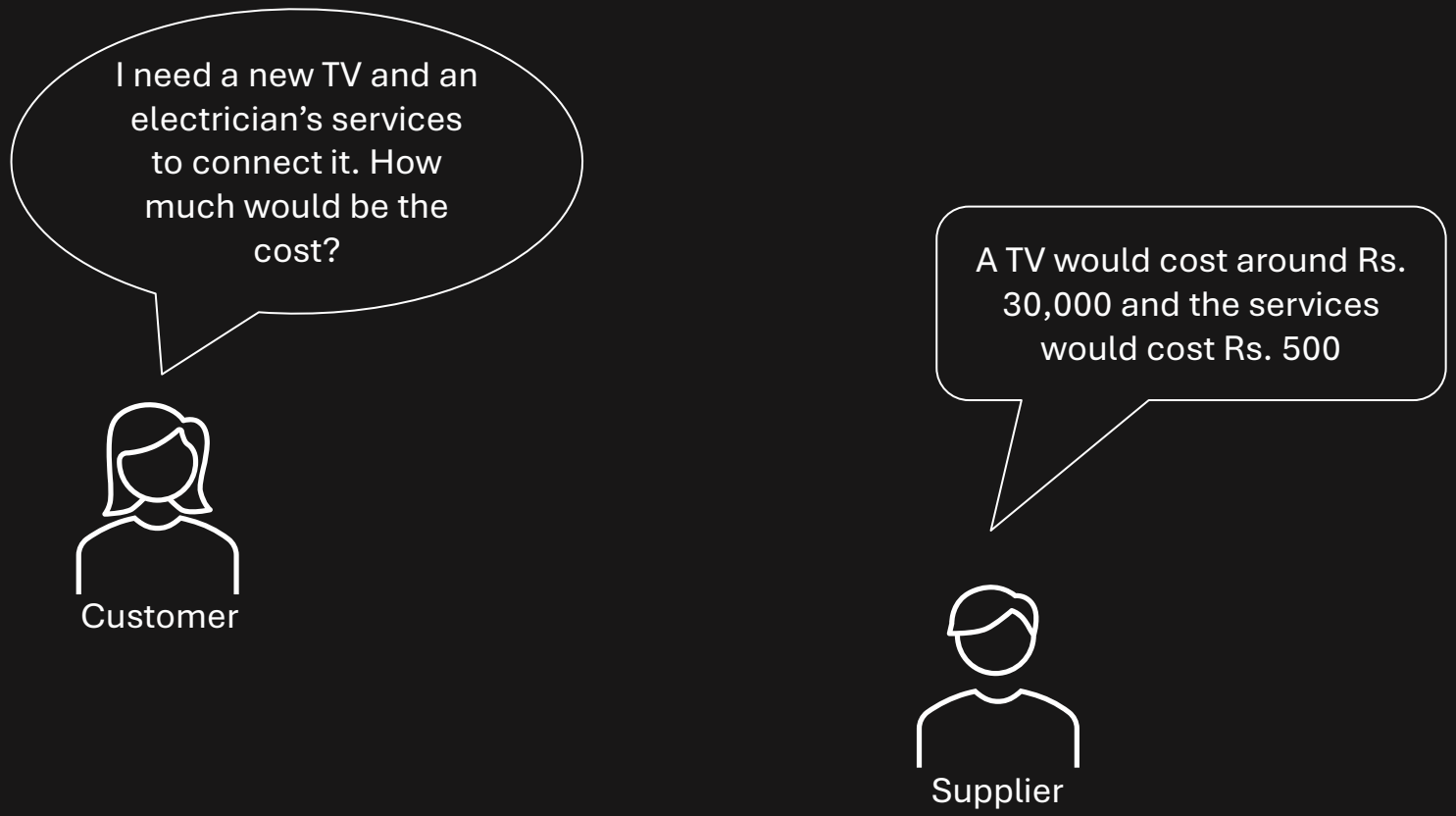
Medium of Exchange



THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

FUNCTIONS OF CURRENCY 3

Unit of Account



THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

MEETING WITH ENGINEERING TEAM

Can you explain a bit more on the forms of money?

Can you please elaborate?

Engineering Manager

Sure. The 1st form is a currency note printed by the central bank. This explicitly establishes the liability of central bank to give you value worth the note you possess

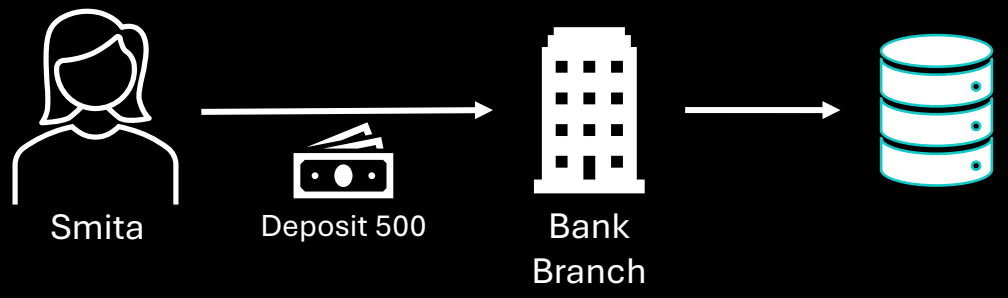
The 2nd form is a record of your balance in a bank's ledger. This is mostly a digital record in current times

Sure. Let's see an example of how these records are maintained

Domain expert

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

DIGITAL LEDGERS



Accounts

User	Balance
Anil	1000
Smita	1000

Balance sheet

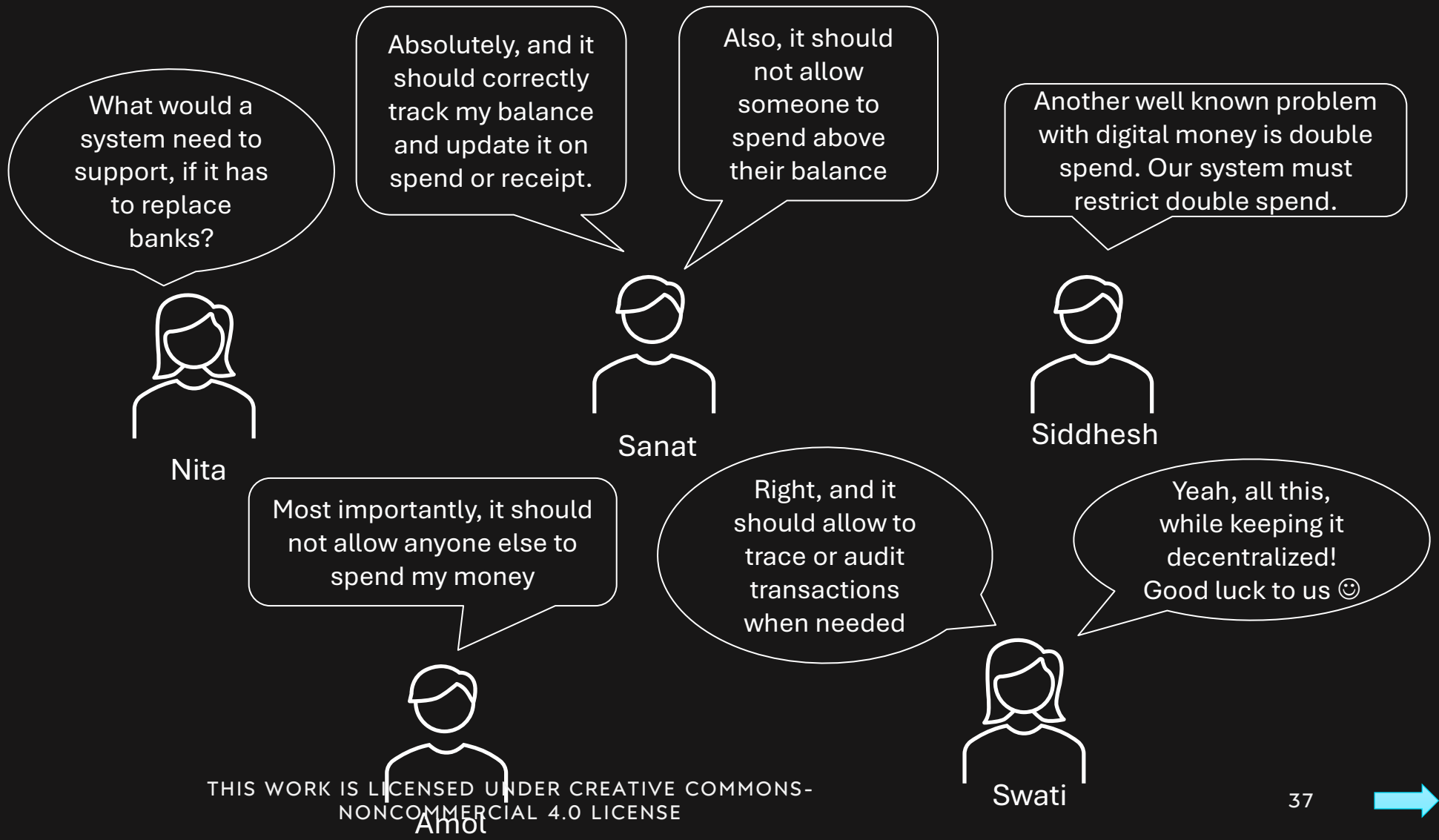
Head	Amount
Assets	
Cash	2000
Liability	
SB Acc	2000

- Account balances are only numbers maintained in bank's databases
- The cash deposited is now an asset for the bank
- Oversight by regulators ensures parity between the accounts and balance sheets minimizing the possibility of malpractice
- But as said, this is a reactive approach. Any wrongdoing would be caught only at the time of audits

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

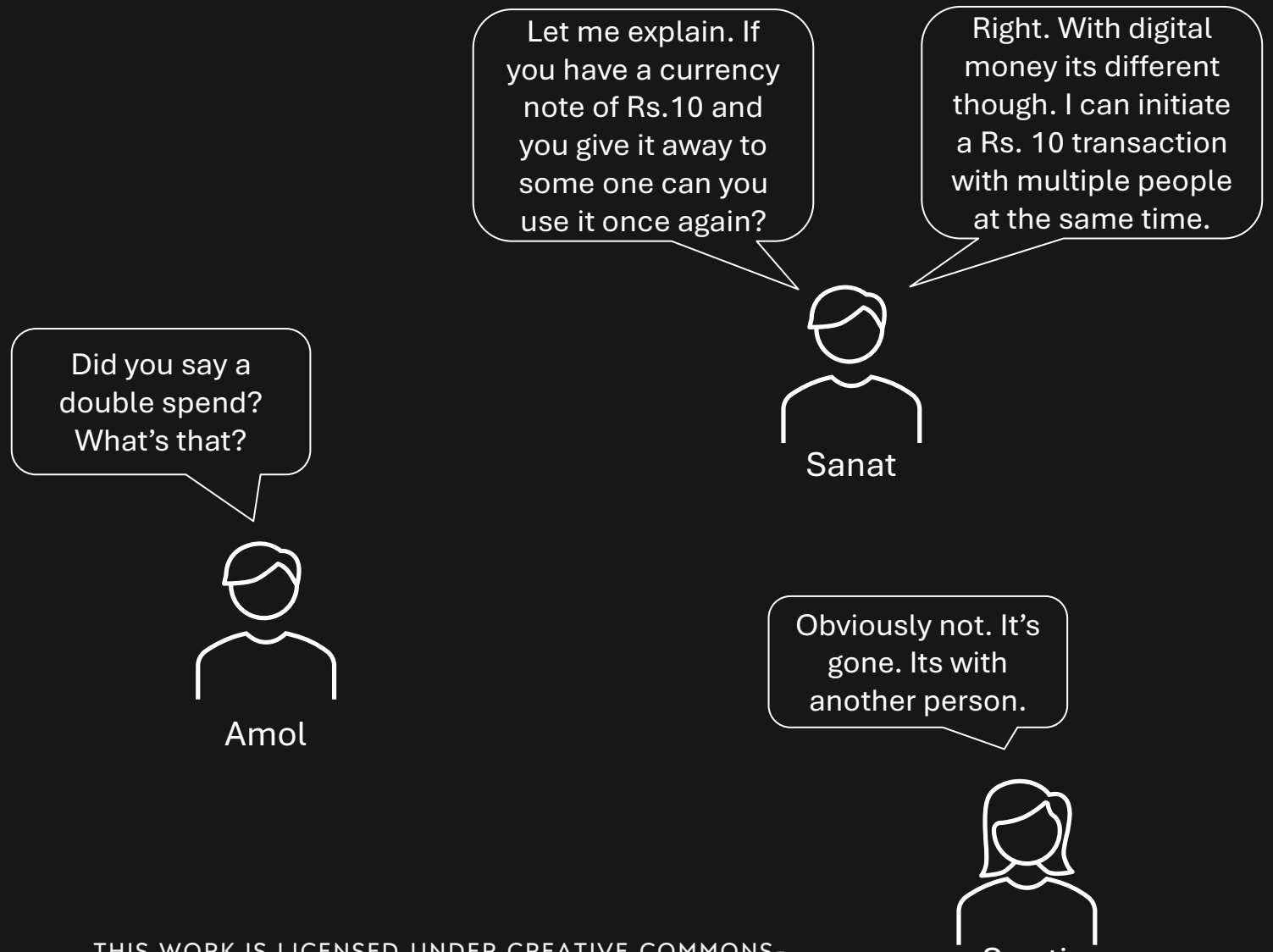
Back to replacing the banks...

SOFTWARE ENGINEERS MEETING



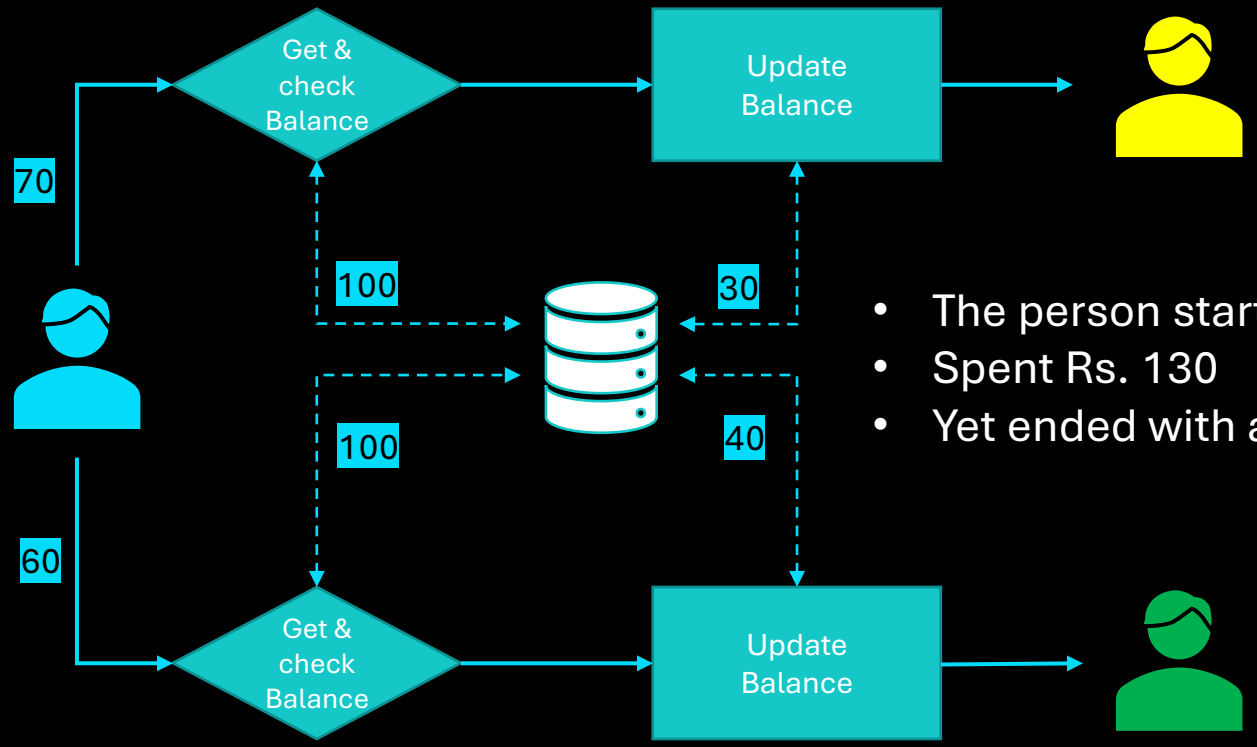
THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

SOFTWARE ENGINEERS MEETING



THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

DOUBLE SPEND – DEEPER DIVE



- The person started with Rs. 100
- Spent Rs. 130
- Yet ended with a balance of Rs. 40

- Transactions cannot execute in parallel
- Transaction order is critical

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

THE NEW SYSTEM REQUIREMENTS

I MUST OWN MY DATA

- Spending rights are only with the owner
- Censorship resistant
- Highly available

ALWAYS IN SYNC TRANSACTION RECORDS

- Any transaction updates the system state across all participants
- This state is used as base for all future transactions

IMMUTABLE RECORDS

- A transaction once done cannot be modified or reversed by anyone

AUDITABILITY

- A trail of transactions is available for audit and scrutiny when needed

COST EFFECTIVE

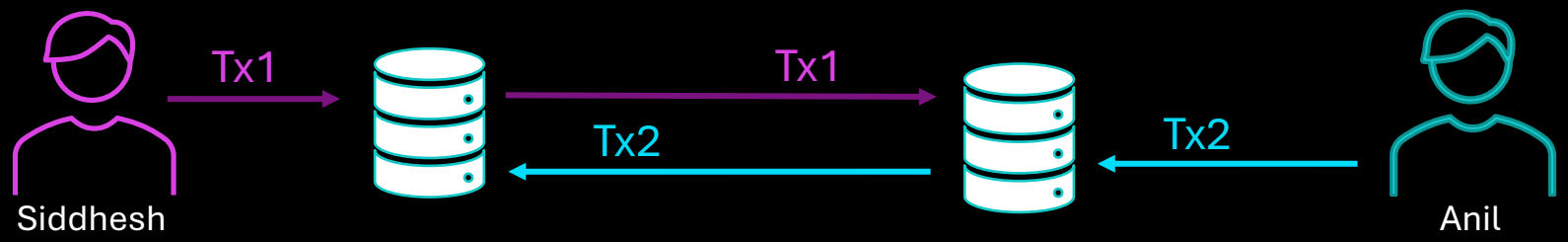
- Cost of a transaction should be competitive as compared to the current centralized payment systems

DOUBLE SPEND RESISTANT

- Should not allow double spend of the currency

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

BRICK 1 – OWN & IN-SYNC DATABASES



Tx	From	To	Amount
1	Siddhesh	Anil	5000
2	Anil	Siddhesh	3500

User	Balance
Anil	1500
Siddhesh	6500

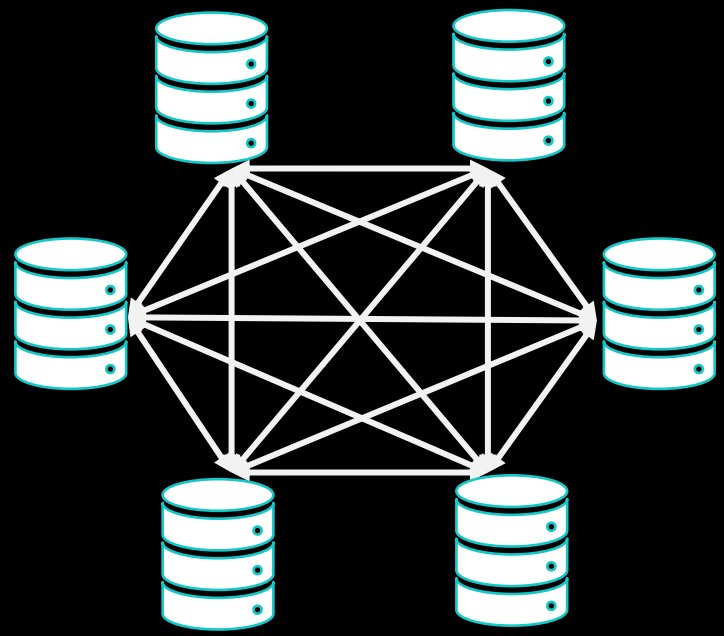
Tx	From	To	Amount
1	Siddhesh	Anil	5000
2	Anil	Siddhesh	3500

User	Balance
Anil	1500
Siddhesh	6500

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

That looks like a distributed database to me. What's the difference?

BRICK 2 – P2P COMMUNICATION



User	Balance
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
Siddhesh	6500

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

Can this be a simple database replication?

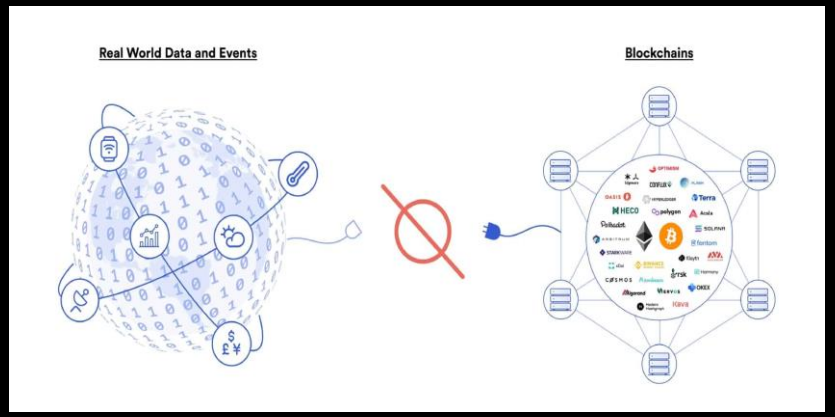
BRICK 3 – EVALUATE, THEN ACCEPT

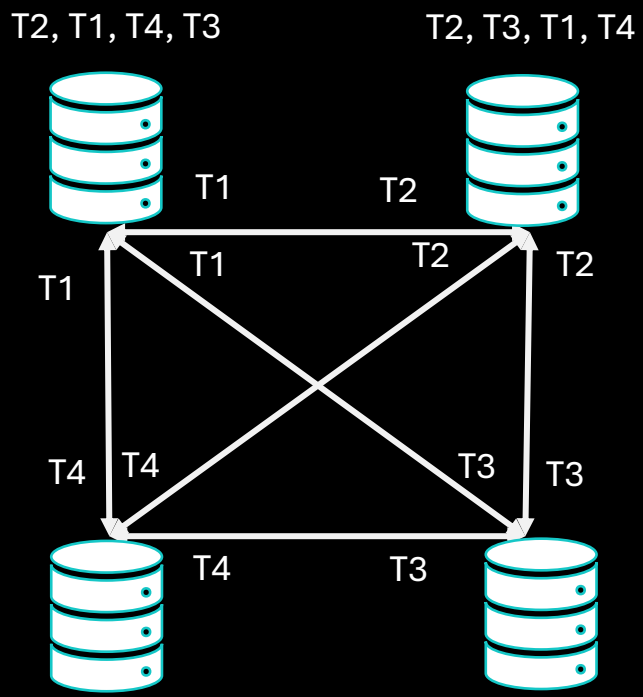
- Is the sender authenticated?
- Does the sender have enough balance?
- Has the sender sent the amount multiple times?
- Is the receiver eligible to receive the money?

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

How do we guarantee that all evaluations lead to same conclusion?

BRICK 4 – DETERMINISM



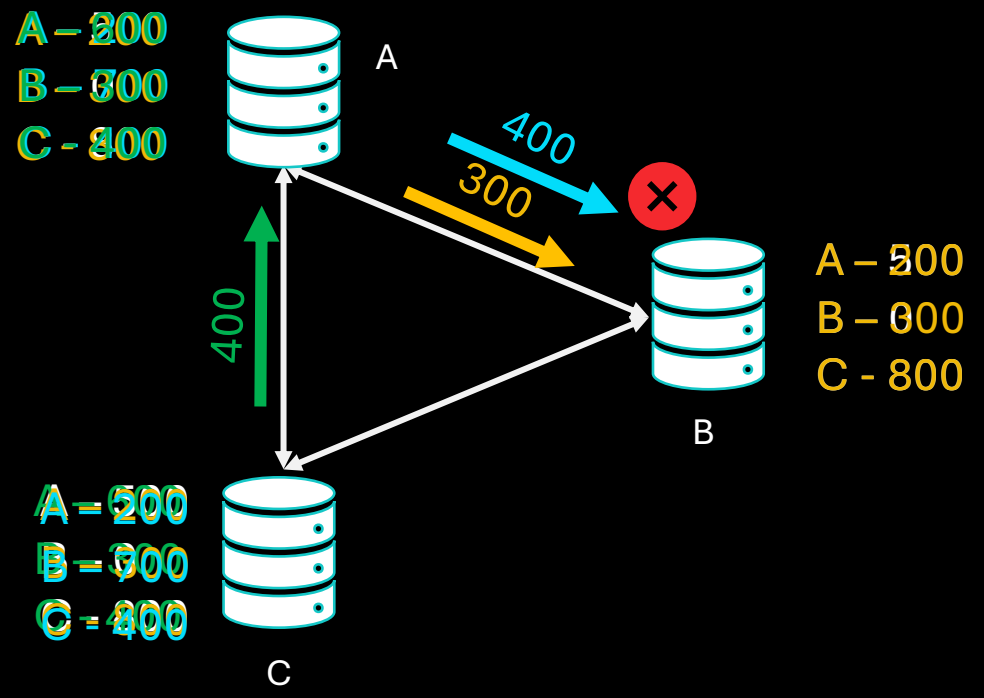


The term Determinism in Computer Science refers to a system where the future state of the system is entirely determined by the prior state and the current operation.
Determinism means that we reach the same state as everybody else if we enact the same operational steps in the same order. This property makes a blockchain what it is.

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

I don’t understand this problem of order of transactions. Why not process transactions as they come in?

BRICK 5 – ORDERING



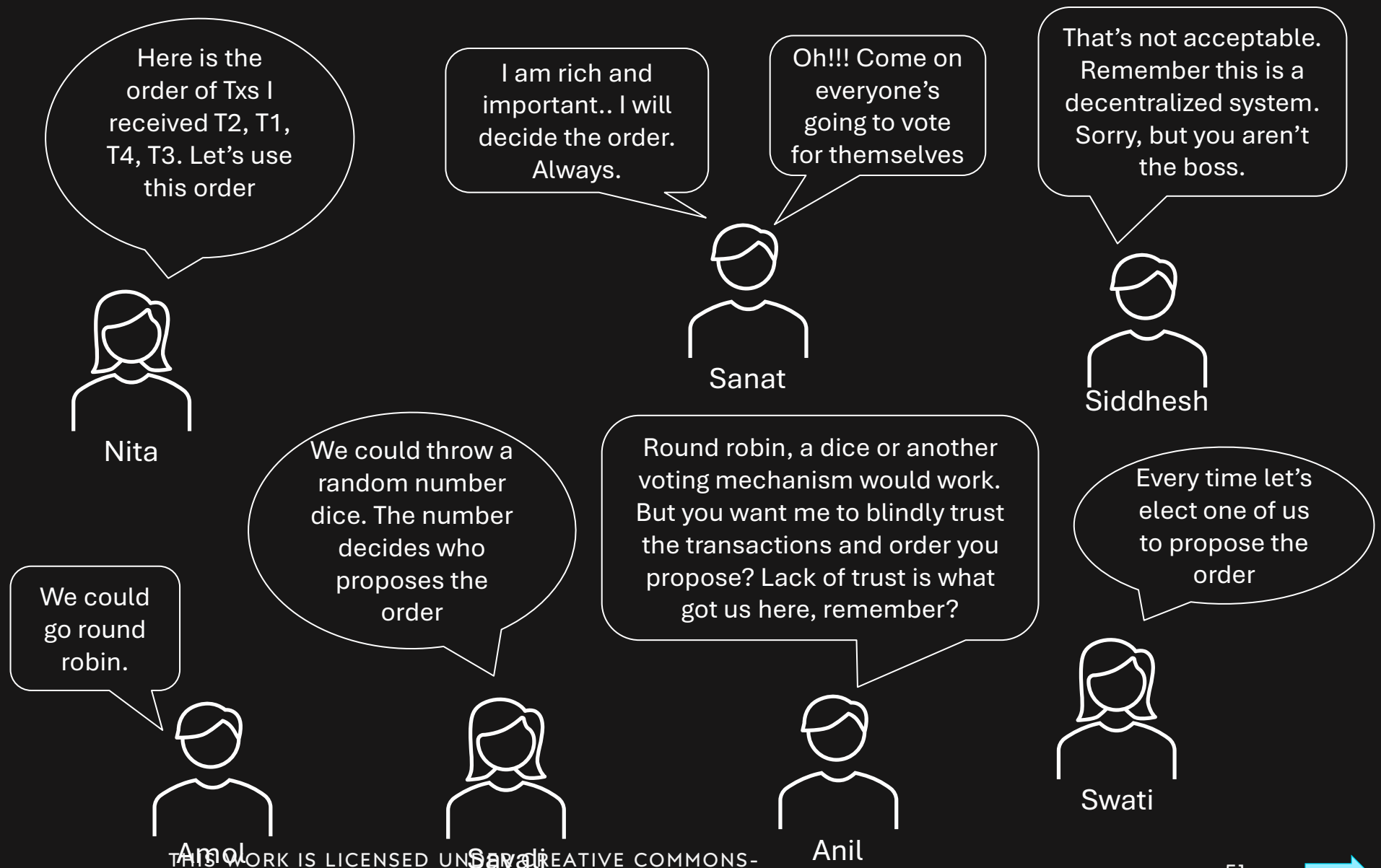
Who is right and who is wrong?

… and this is just a trailer of how bad things can get

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

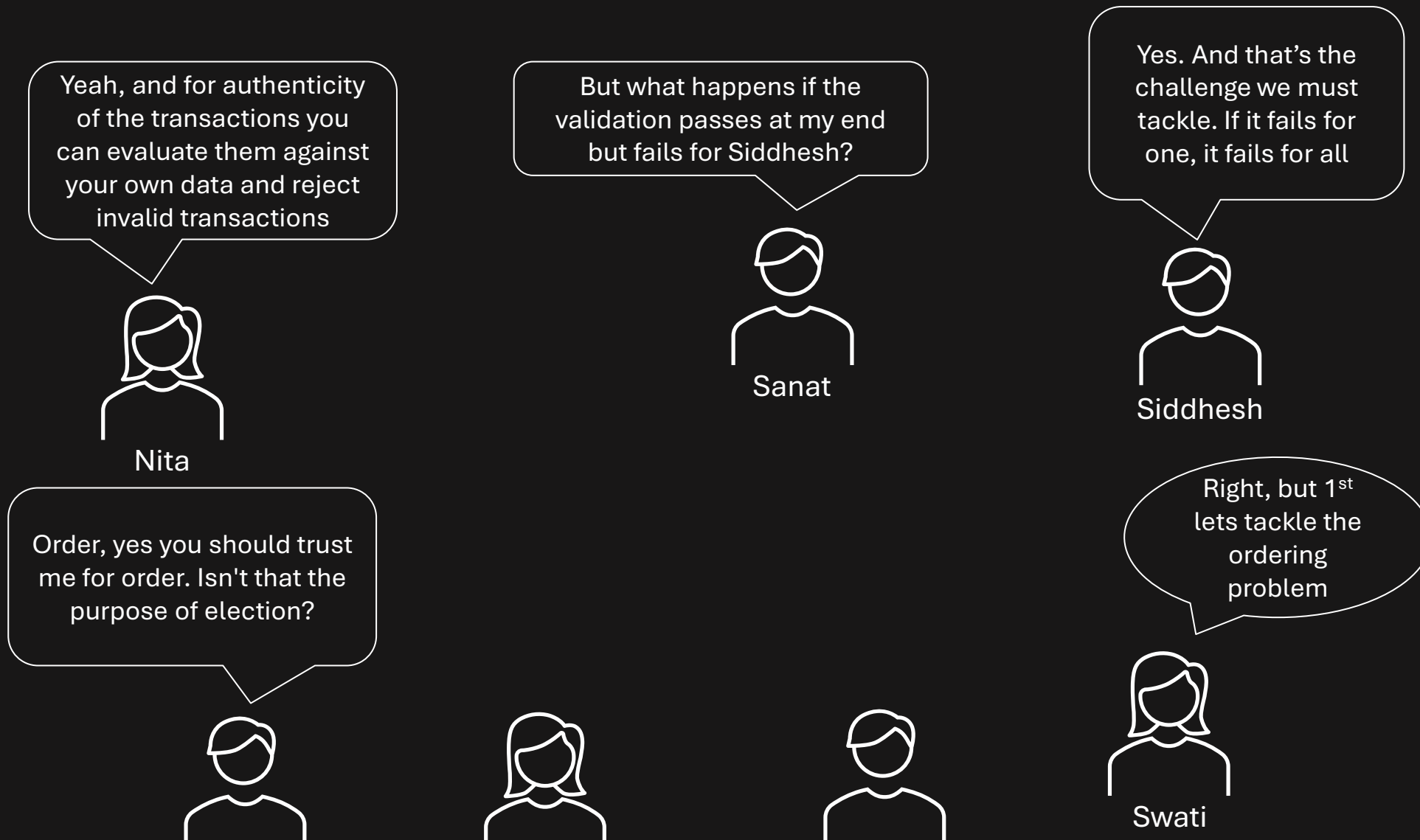
Interesting. If the system is decentralized, who decides the order?

AN ORDERING CONUNDRUM



THIS WORK IS LICENSED UNDER A CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

AN ORDERING CONUNDRUM



THIS WORK IS LICENSED UNDER A CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

THE CONSENSUS

POW

Proof of work (PoW) is a form of cryptographic proof in which one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended. Verifiers can subsequently confirm this expenditure with minimal effort on their part. The concept was invented by Moni Naor and Cynthia Dwork in 1993 as a way to deter denial-of-service attacks and other service abuses such as spam on a network by requiring some work from a service requester, usually meaning processing time by a computer.

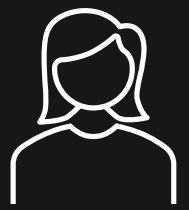
POS

Proof-of-stake (PoS) protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency. This is done to avoid the computational cost of proof-of-work (POW) schemes.

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE

MANY MORE CONCERNS STILL

So, we all agree we need an algorithm/mechanism to decide who proposes order



Nita

But will these algorithms propose one transaction to commit at a time? That will be lot of computation and Tx backlog. The system will be extremely slow.

Sanat

How do I even trust that the transactions are coming from one of you? You can very well deny sending the transaction later

Sayali

... yeah, we could change the order too.

Anil

We are still using databases though. What stops any of us from changing data in there?

Swati

THIS WORK IS LICENSED UNDER CREATIVE COMMONS NONCOMMERCIAL 4.0 LICENSE

- Also does every payer and payee need to deploy a node now? That’s just unthinkable.
- Then which node does a user connect to?
- If a user can connect to any node, it means my money, my balance is available on all nodes. Where is the much needed privacy?

THANK YOU

THIS WORK IS LICENSED UNDER CREATIVE COMMONS-NONCOMMERCIAL 4.0 LICENSE