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.

AGENDA

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

SCENE 1 – THE CREDIT SALE

Through the month

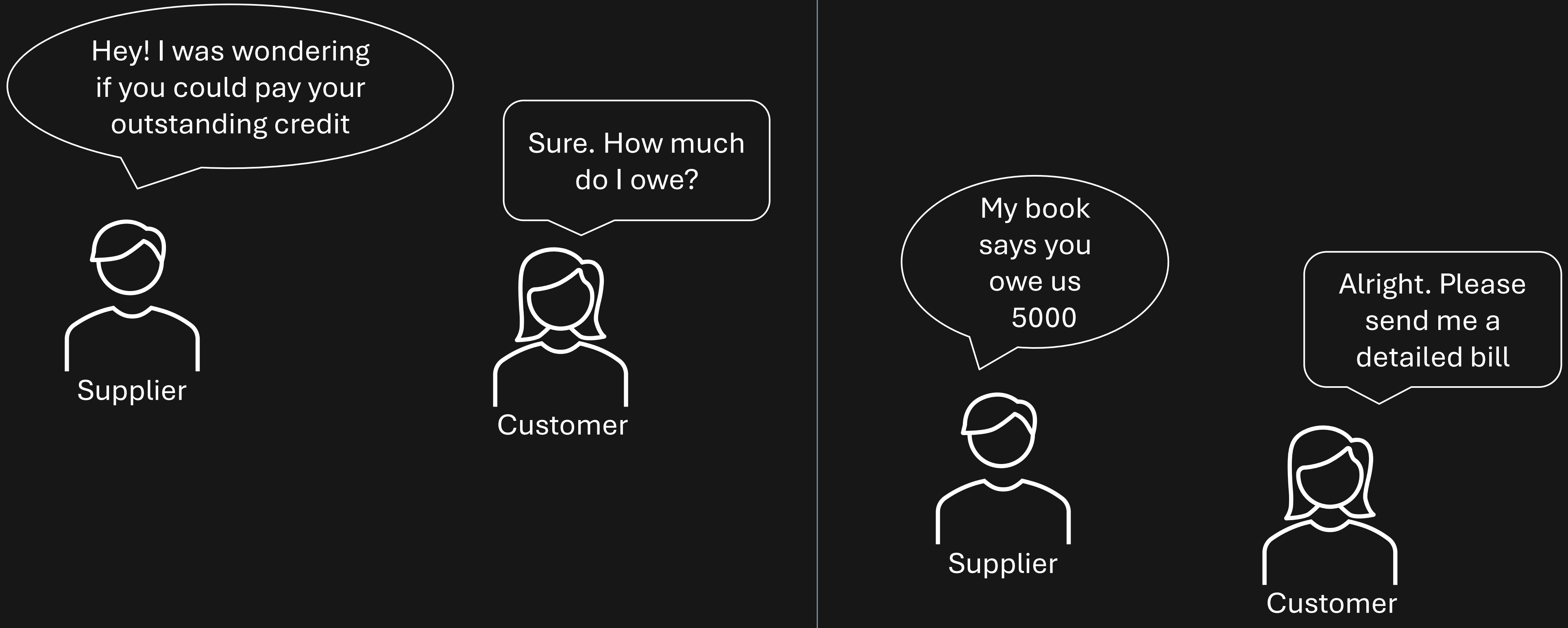
Can you please put my purchase on credit?
Customer
Absolutely.
Supplier
Thanks a ton
Customer
You bet.
Supplier

Supplier maintains the records

SCENE 1 – THE CREDIT SALE

Supplier maintains the records

31st of the month



Hey! I was wondering if you could pay your outstanding credit

Supplier

Sure. How much do I owe?

Customer

My book says you owe us 5000

Supplier

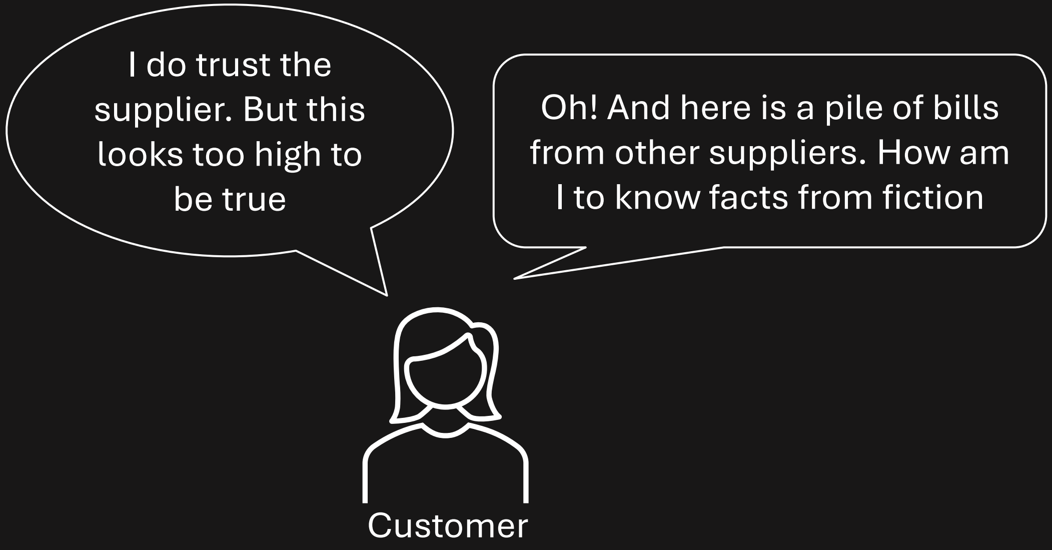
Alright. Please send me a detailed bill

Customer

SCENE 1 – THE CREDIT SALE

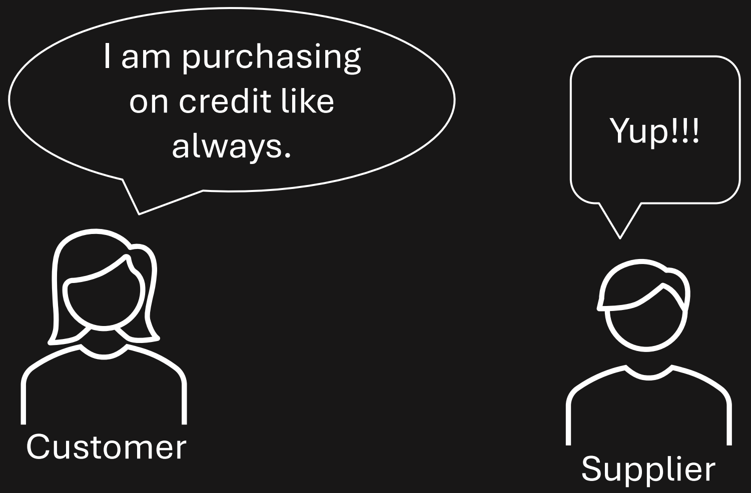
Supplier maintains the records

On receipt of the bills

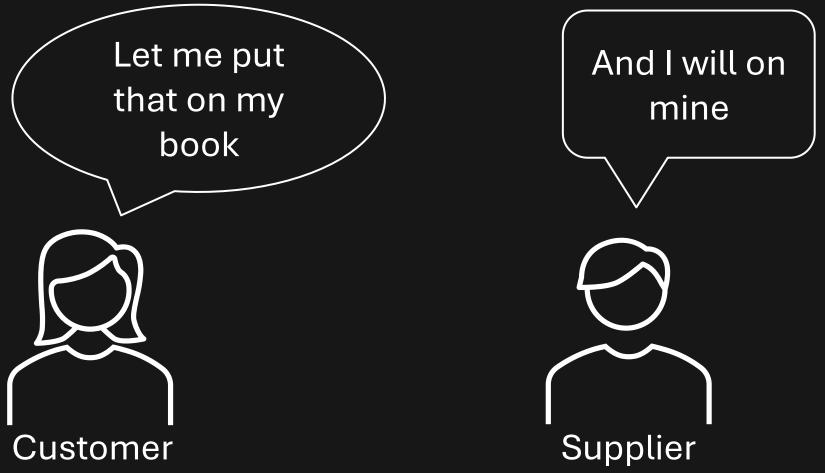

I do trust the supplier. But this looks too high to be true
Oh! And here is a pile of bills from other suppliers. How am I to know facts from fiction
Customer

How do we solve this?

SCENE 2 – THE CREDIT SALE



Through the month

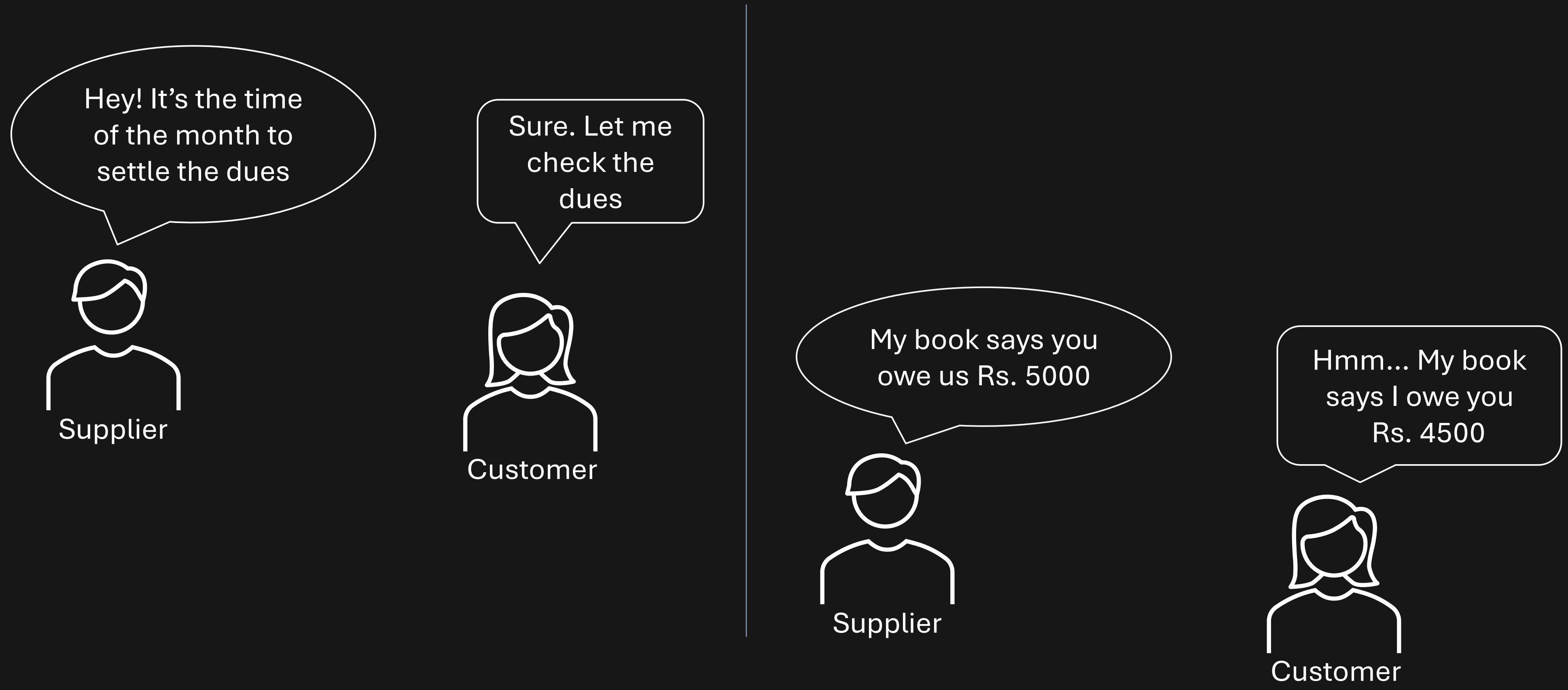


Supplier & Customer maintain their own records

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records

31st of the month


Hey! It’s the time of the month to settle the dues
Supplier
Sure. Let me check the dues
Customer
My book says you owe us Rs. 5000
Supplier
Hmm... My book says I owe you Rs. 4500
Customer

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records

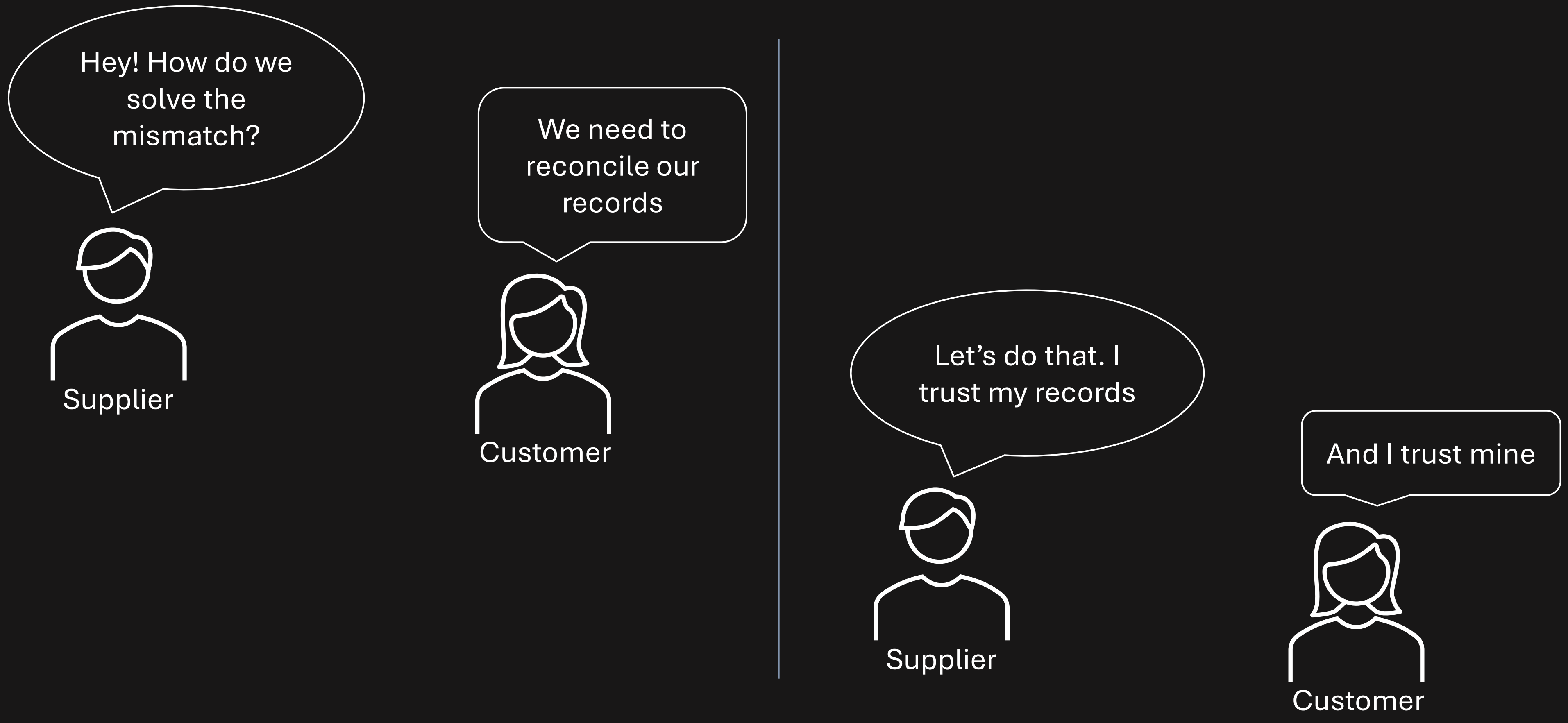
A few moments later

My suspicion seems to be true. Something's wrong with his accounts.
Customer

SCENE 2 – THE CREDIT SALE

Supplier & Customer maintain their own records

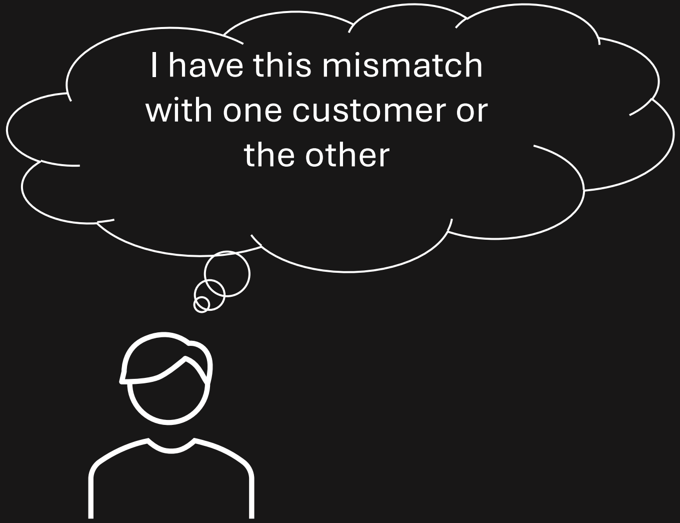
After a few days


Hey! How do we solve the mismatch?
Supplier
We need to reconcile our records
Customer
Let’s do that. I trust my records
Supplier
And I trust mine
Customer

SCENE 2 – THE CREDIT SALE

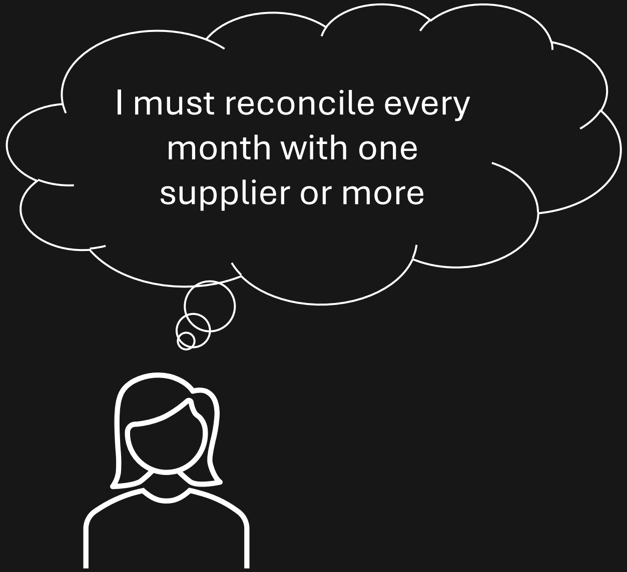
Supplier & Customer maintain their own records

Every month



I have this mismatch with one customer or the other

Supplier

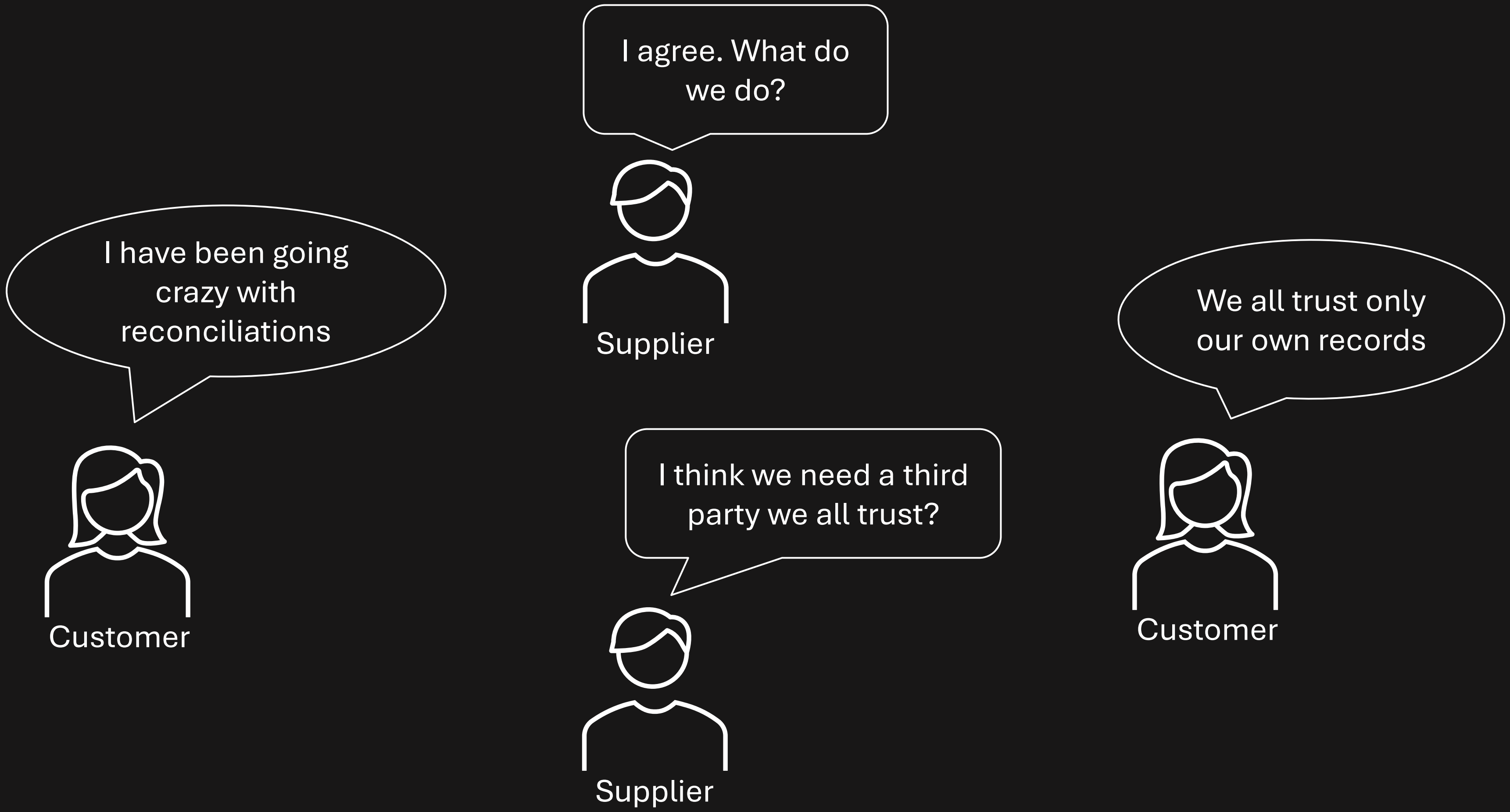


I must reconcile every month with one supplier or more

Customer

How do we fix this?

SCENE 3 –SUPPLIER CUSTOMER CONF


I have been going crazy with reconciliations
Customer
I agree. What do we do?
Supplier
We all trust only our own records
Customer
I think we need a third party we all trust?
Supplier

Let's get an intermediary

SCENE 3 –THE INTERMEDIARY

Let’s meet our intermediary

Glad and relieved to hear that

Supplier

Yup! Here is the signed agreement

When can you start?

Customer

Supplier

Hi Folks, I am your new record keeper. You can trust me. My processes are ISO certified.

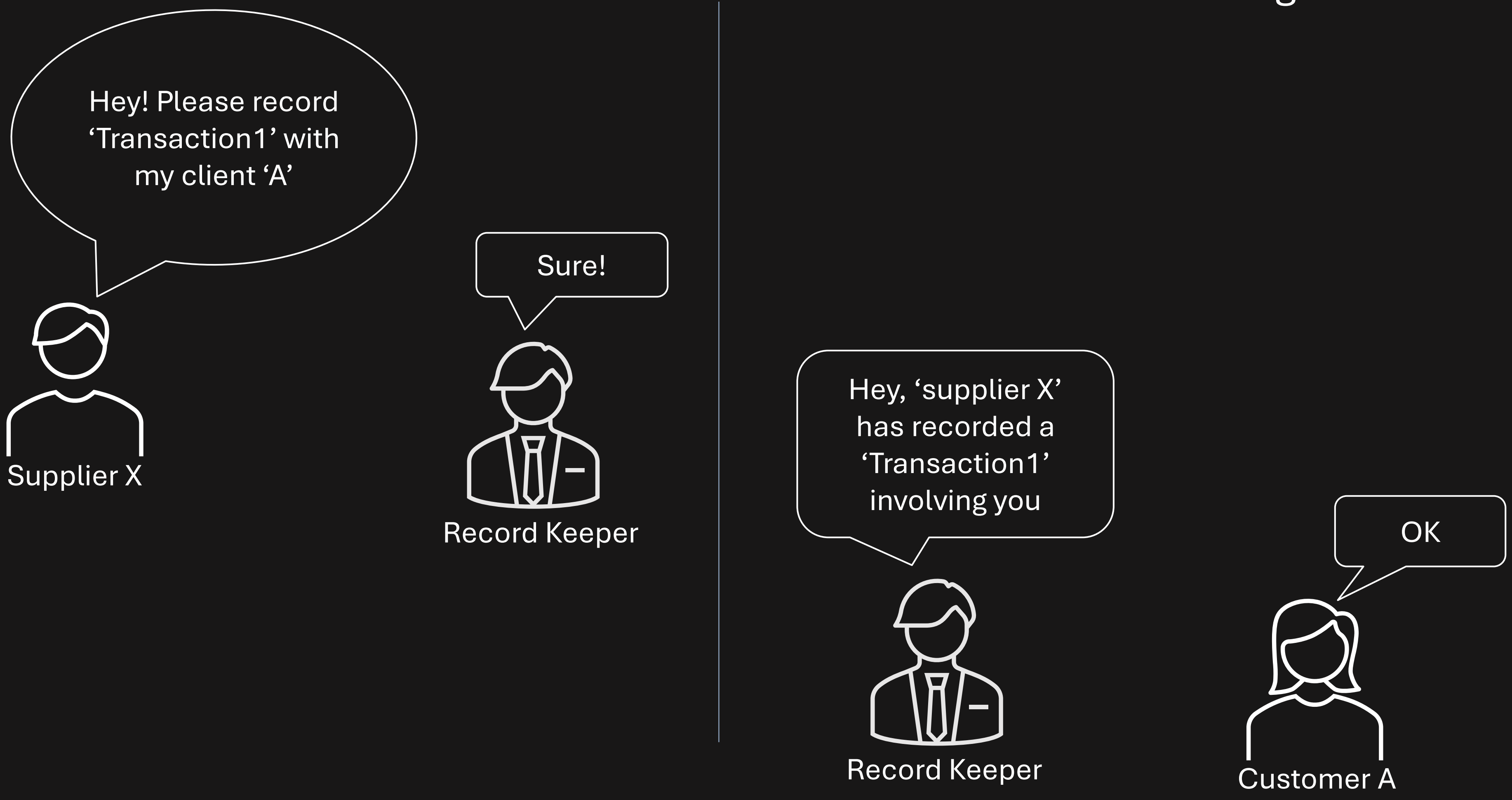
As soon as you have signed the agreement

Record Keeper

SCENE 3 – THE CREDIT SALE

Transacting with the help of intermediary

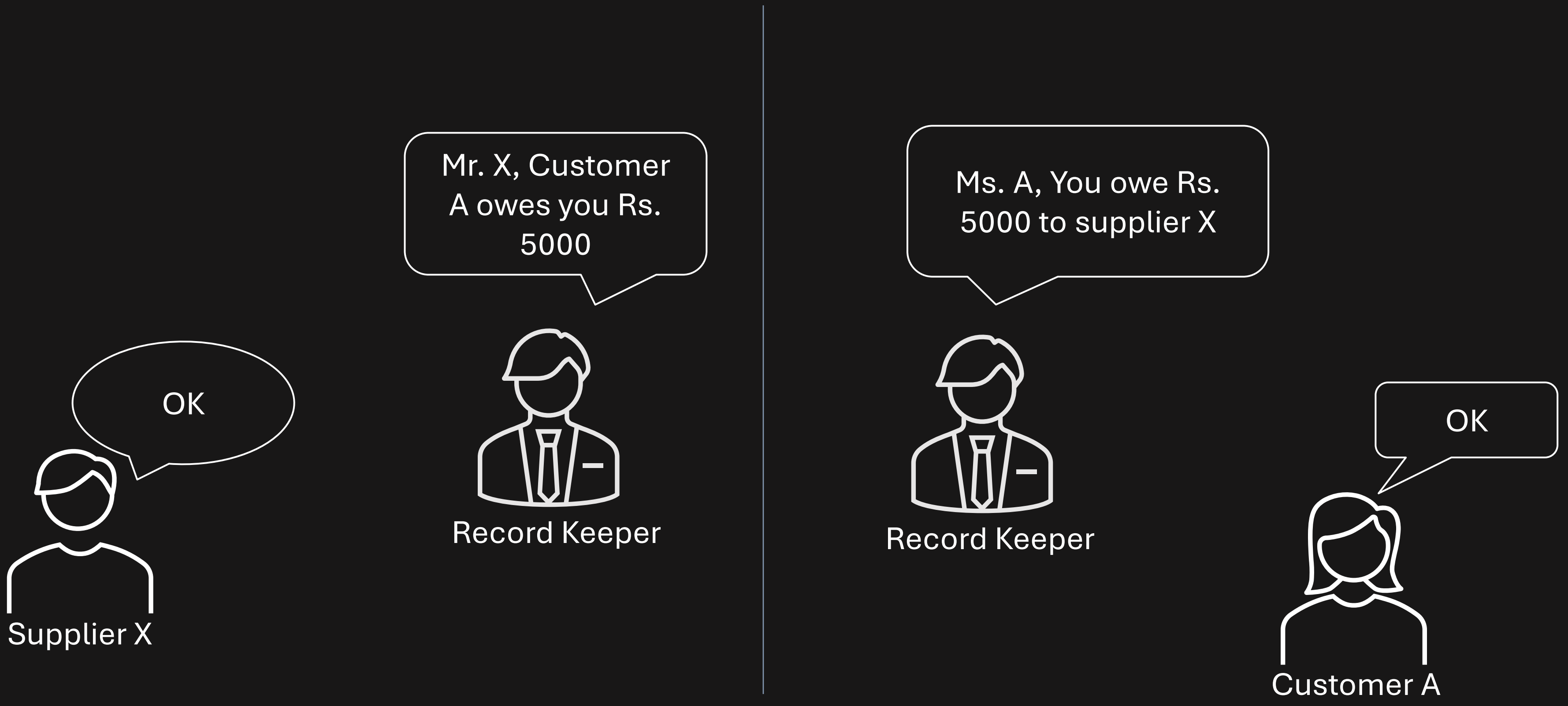
Through the month


Hey! Please record 'Transaction1' with my client 'A'
Supplier X
Sure!
Record Keeper
Hey, 'supplier X' has recorded a 'Transaction1' involving you
Record Keeper
OK
Customer A

SCENE 3 – THE CREDIT SALE

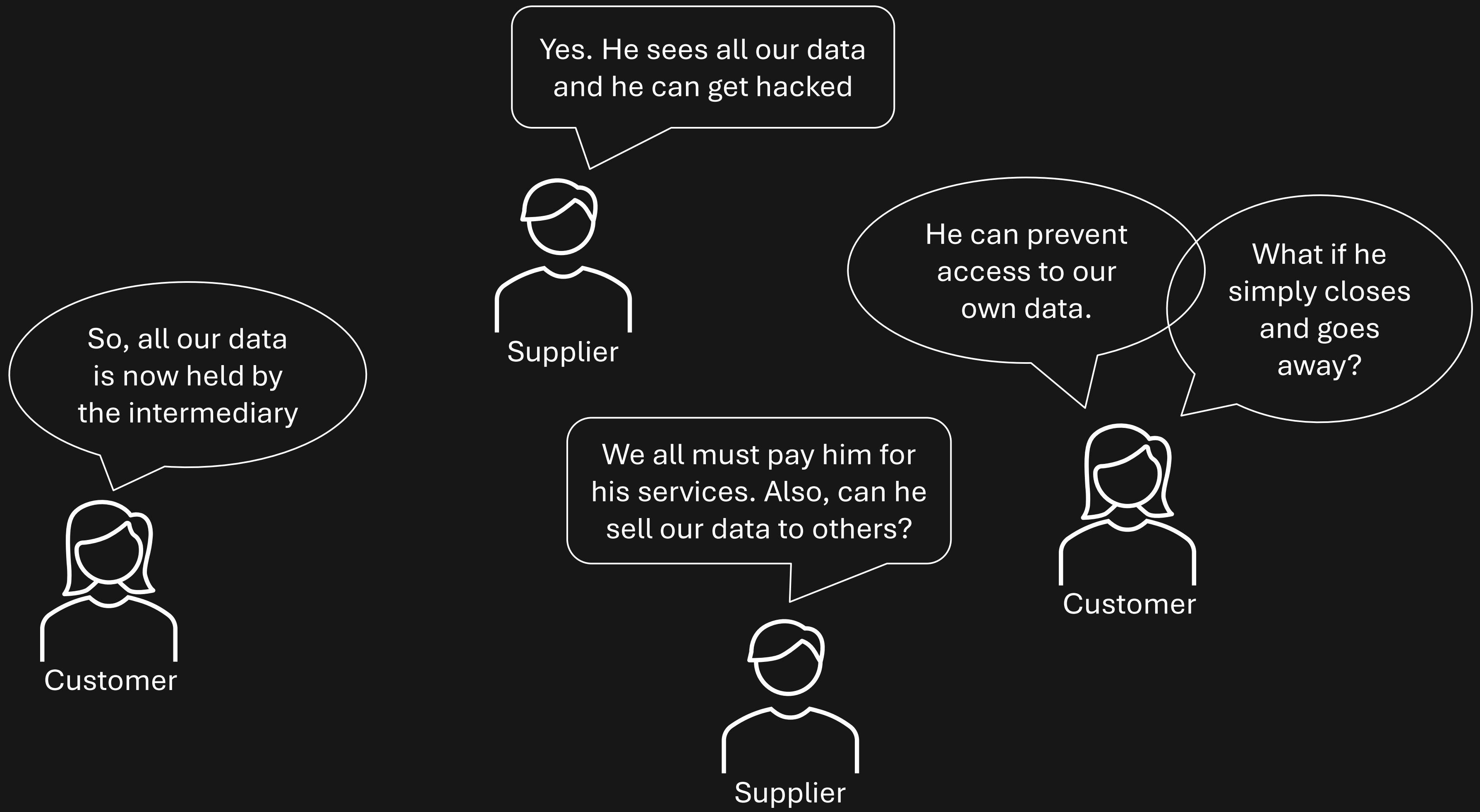
Transacting with the help of intermediary

31st of the month


OK
Supplier X
Mr. X, Customer A owes you Rs. 5000
Record Keeper
Ms. A, You owe Rs. 5000 to supplier X
Record Keeper
OK
Customer A

Can you name some intermediaries?

SCENE 4 – ANNUAL MEETING


So, all our data is now held by the intermediary
Customer
Yes. He sees all our data and he can get hacked
Supplier
We all must pay him for his services. Also, can he sell our data to others?
Supplier
He can prevent access to our own data.
What if he simply closes and goes away?
Customer

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

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

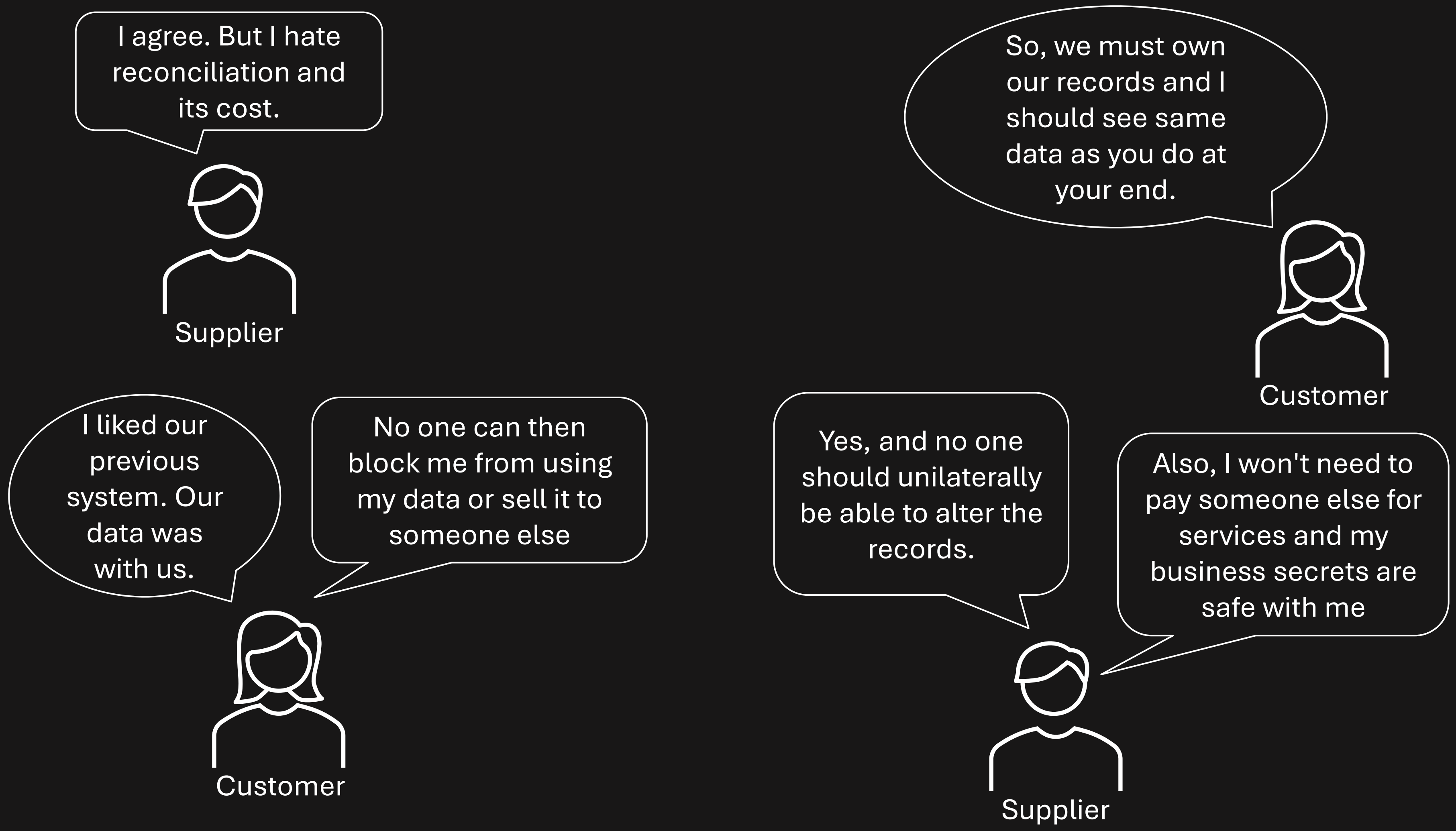
The data collected acts as a honey pot and despite several measures, data breaches are a frequent occurrence

DATA TAMPERING RISK

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

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

SCENE 4 – ANNUAL MEETING



I agree. But I hate reconciliation and its cost.

Supplier

So, we must own our records and I should see same data as you do at your end.

Customer

I liked our previous system. Our data was with us.

No one can then block me from using my data or sell it to someone else

Customer

Yes, and no one should unilaterally be able to alter the records.

Also, I won't need to pay someone else for services and my business secrets are safe with me

Supplier

We need our old system but a new approach

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

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

Hey, my team is trying to imagine a world without banks. I was wondering how can you help?

Alright. Can you explain it to us?

Engineering Manager

I hear you. But do you understand how money works? If not that’s what you will need to do before trying to work out a solution.

Absolutely. Let's jump right in.

Domain expert

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

FUNCTIONS OF CURRENCY -1

Store of Value

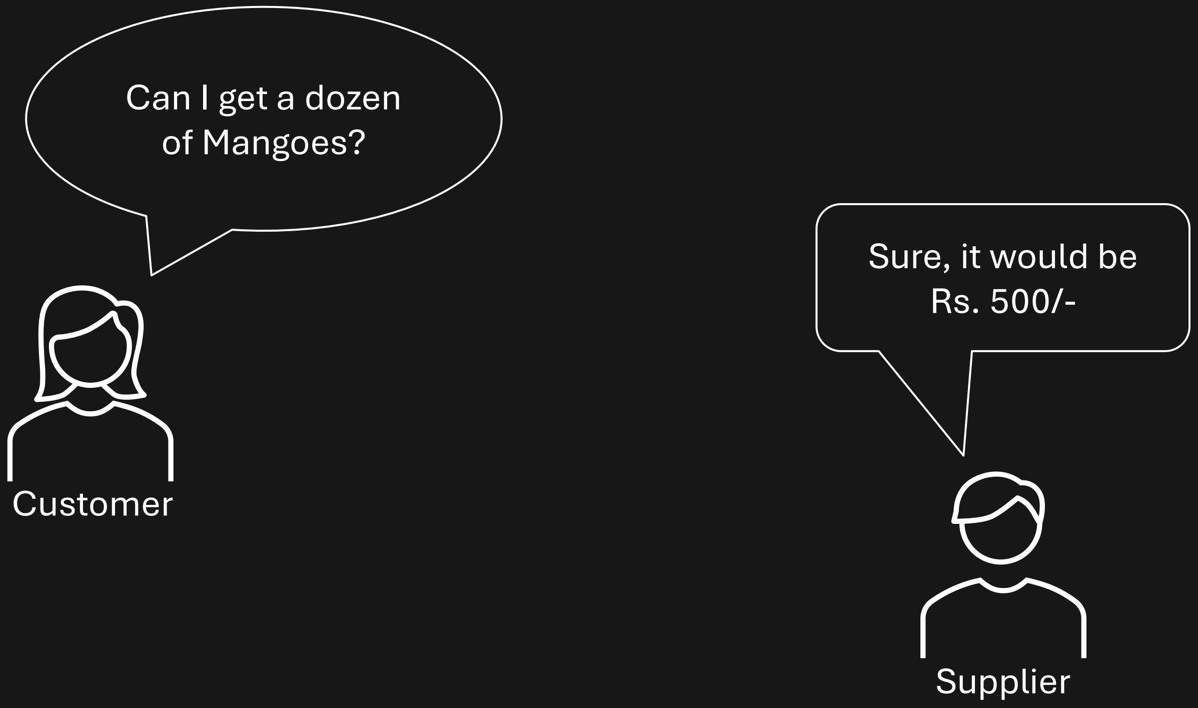
After 3 years

I can buy a car with the 10L Rupees I have

I can still buy a car with the 10L Rupees I have

FUNCTIONS OF CURRENCY 2

Medium of Exchange



Can I get a dozen of Mangoes?

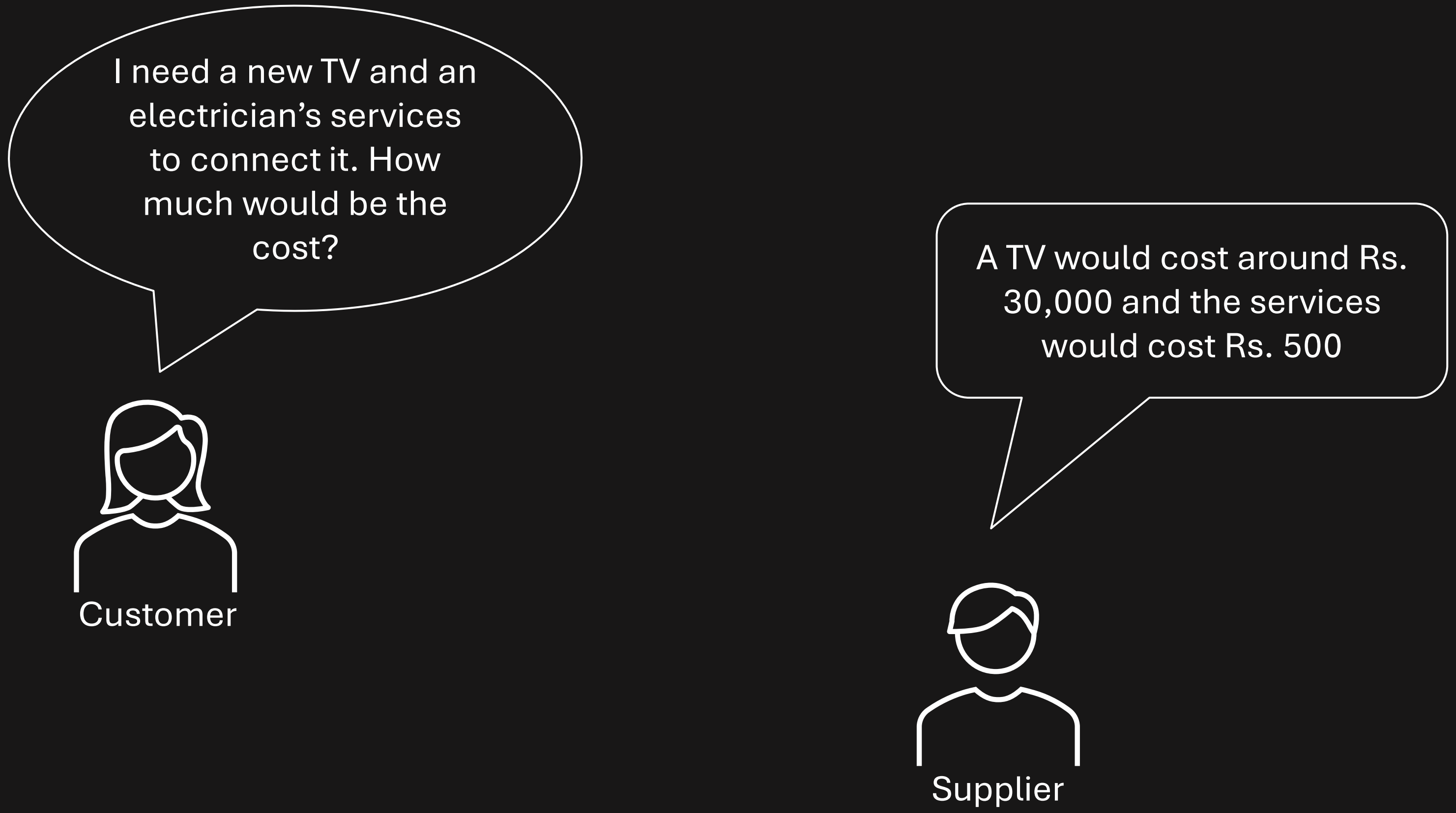
Customer

Sure, it would be Rs. 500/-

Supplier

FUNCTIONS OF CURRENCY 3

Unit of Account



I need a new TV and an electrician's services to connect it. How much would be the cost?

Customer

A TV would cost around Rs. 30,000 and the services would cost Rs. 500

Supplier

MEETING WITH ENGINEERING TEAM

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

Can you please elaborate?

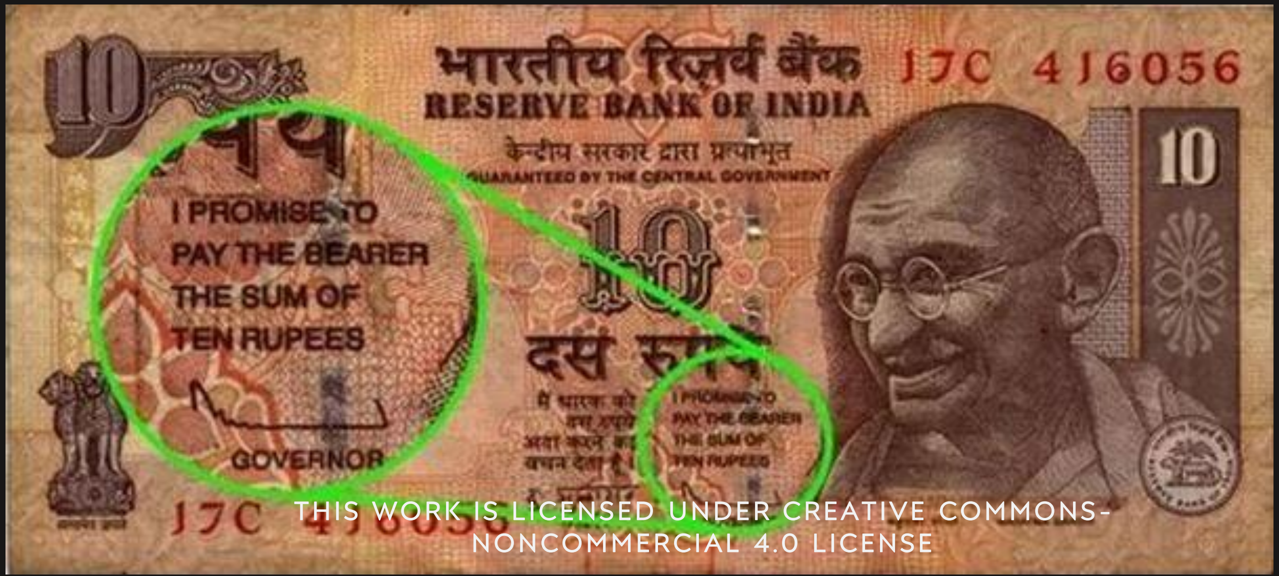
Engineering Manager

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

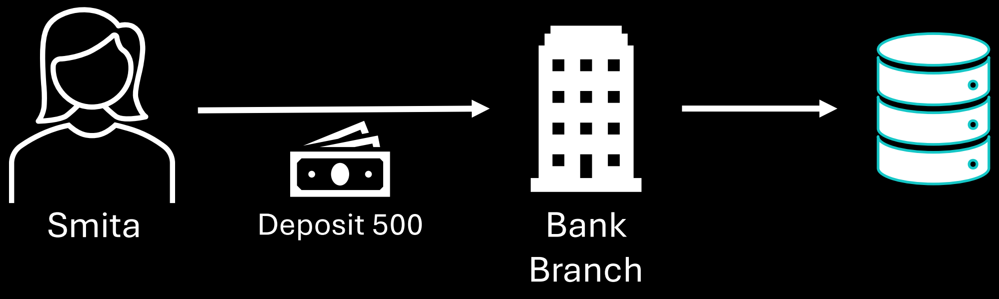
The 2nd form is a record of your balance in a bank's ledger. This is mostly a digital record in current times

Domain expert

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


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
J7C 416056
केन्द्रीय सरकार द्वारा प्रत्याभूत
GUARANTEED BY THE CENTRAL GOVERNMENT
10
I PROMISE TO PAY THE BEARER THE SUM OF TEN RUPEES
दस रुपये
GOVERNOR

DIGITAL LEDGERS



Accounts

User	Balance
Anil	1000
Smita	1000

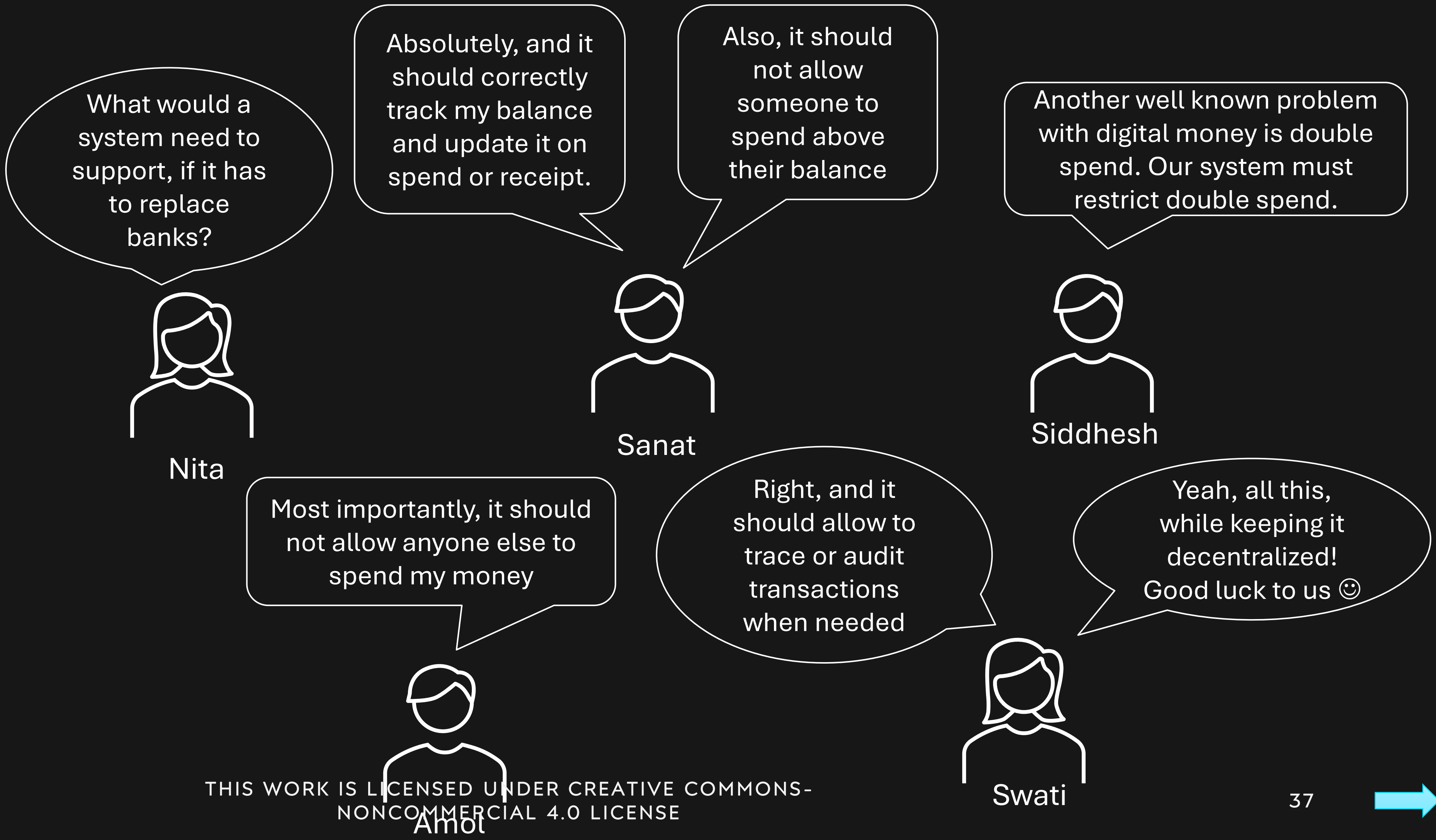
Balance sheet

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

Back to replacing the banks...

SOFTWARE ENGINEERS MEETING



What would a system need to support, if it has to replace banks?

Nita

Absolutely, and it should correctly track my balance and update it on spend or receipt.

Also, it should not allow someone to spend above their balance

Sanat

Another well known problem with digital money is double spend. Our system must restrict double spend.

Siddhesh

Most importantly, it should not allow anyone else to spend my money

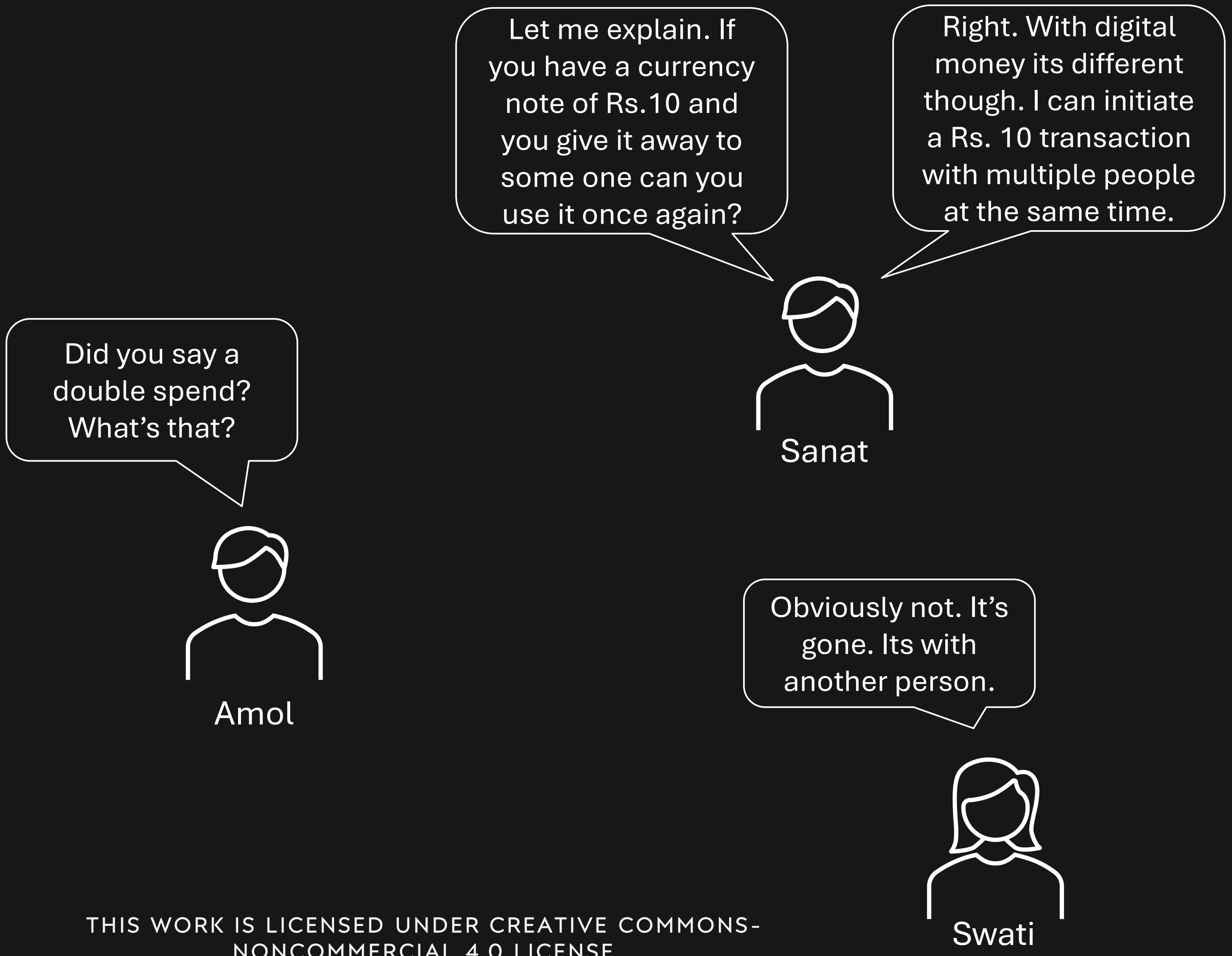
Amol

Right, and it should allow to trace or audit transactions when needed

Yeah, all this, while keeping it decentralized! Good luck to us ☺

Swati

SOFTWARE ENGINEERS MEETING



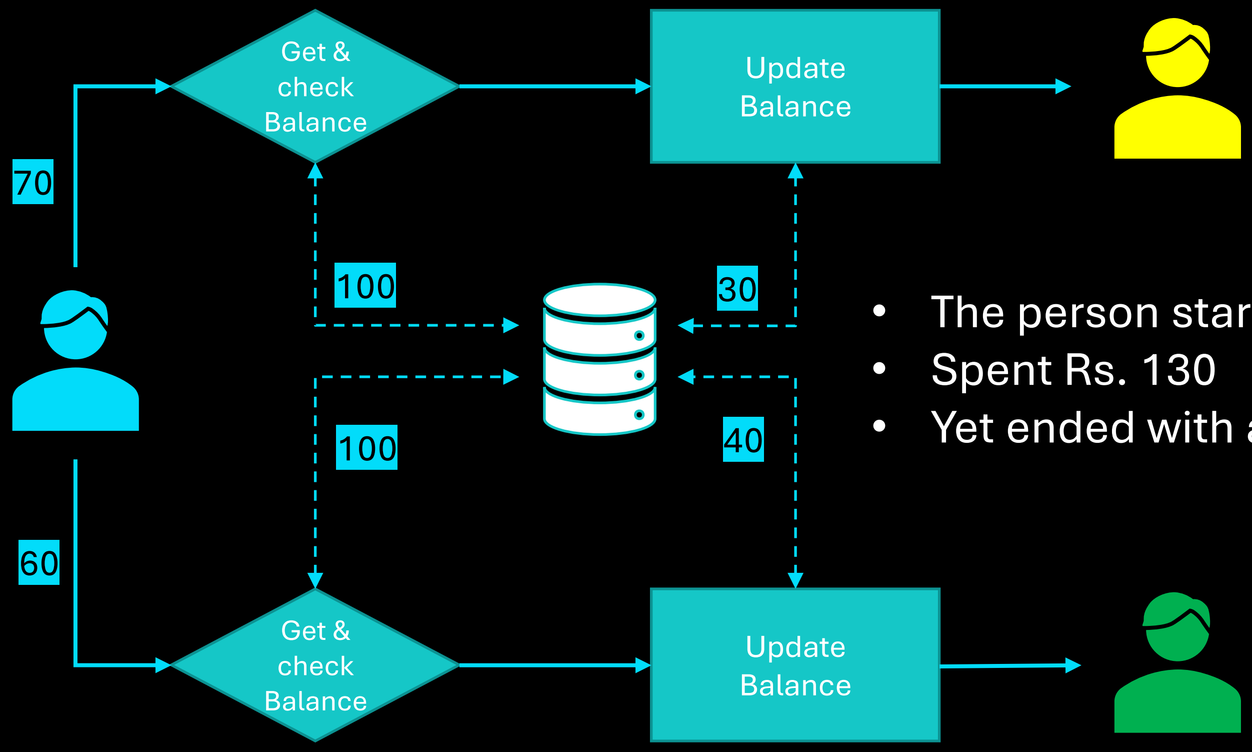
Amol: Did you say a double spend? What's that?

Sanat: Let me explain. If you have a currency note of Rs.10 and you give it away to some one can you use it once again?

Swati: Obviously not. It's gone. Its with another person.

Sanat: Right. With digital money its different though. I can initiate a Rs. 10 transaction with multiple people at the same time.

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

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

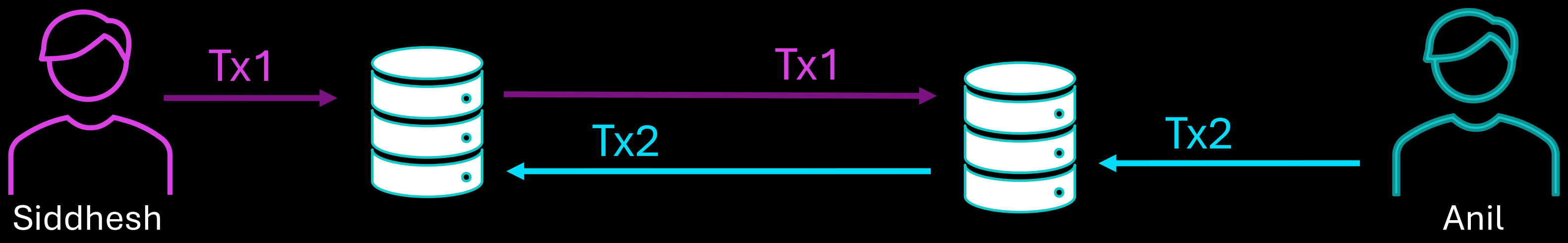
COST EFFECTIVE

- 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

BRICK 1 – OWN & IN-SYNC DATABASES



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

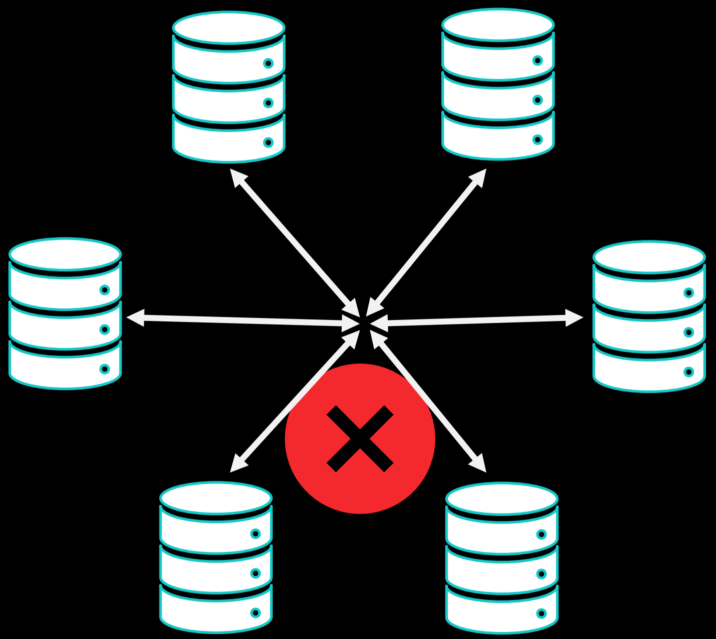
Tx	From	To	Amount
1	Siddhesh	Anil	5000
2	Anil	Siddhesh	3500

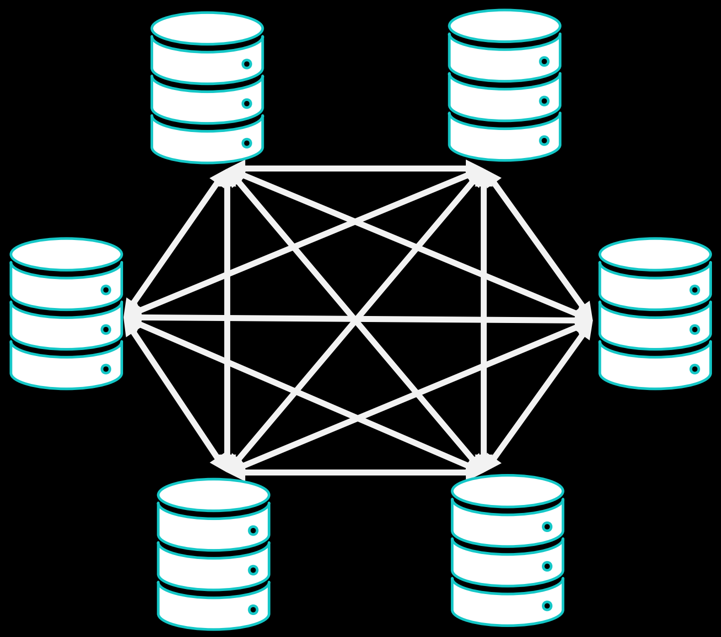
User	Balance
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
Siddhesh	6500

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

BRICK 2 – P2P COMMUNICATION





User	Balance
Anil	1500
Siddhes	

User	Balance
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
iddhesh	6500

er	Balance
	1500
Siddhesh	6500

User	
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
Siddhesh	6500

User	Balance
Anil	1500
Siddhesh	6500

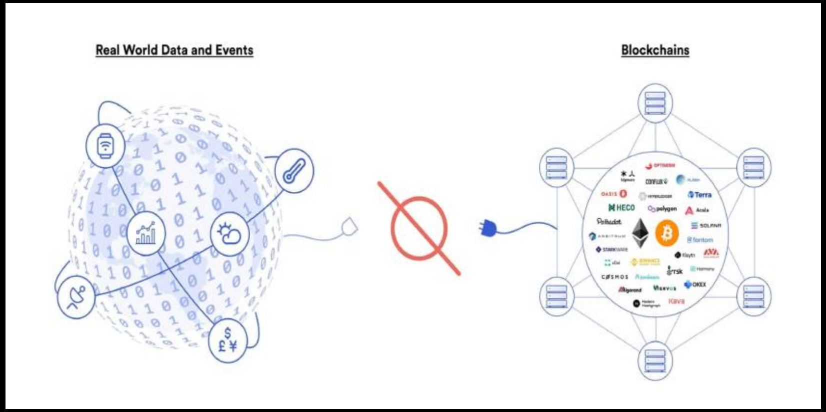
Can this be a simple database replication?

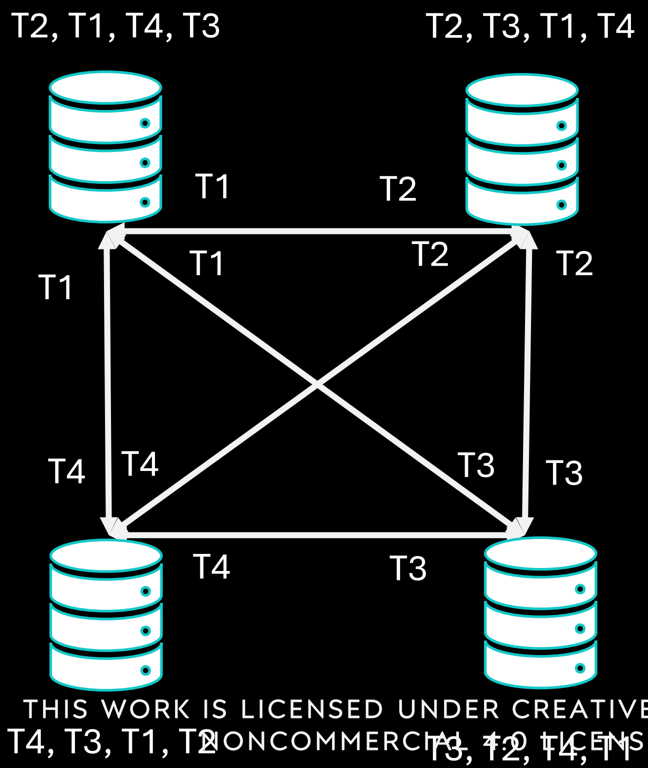
BRICK 3 – EVALUATE, THEN ACCEPT

- 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?

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

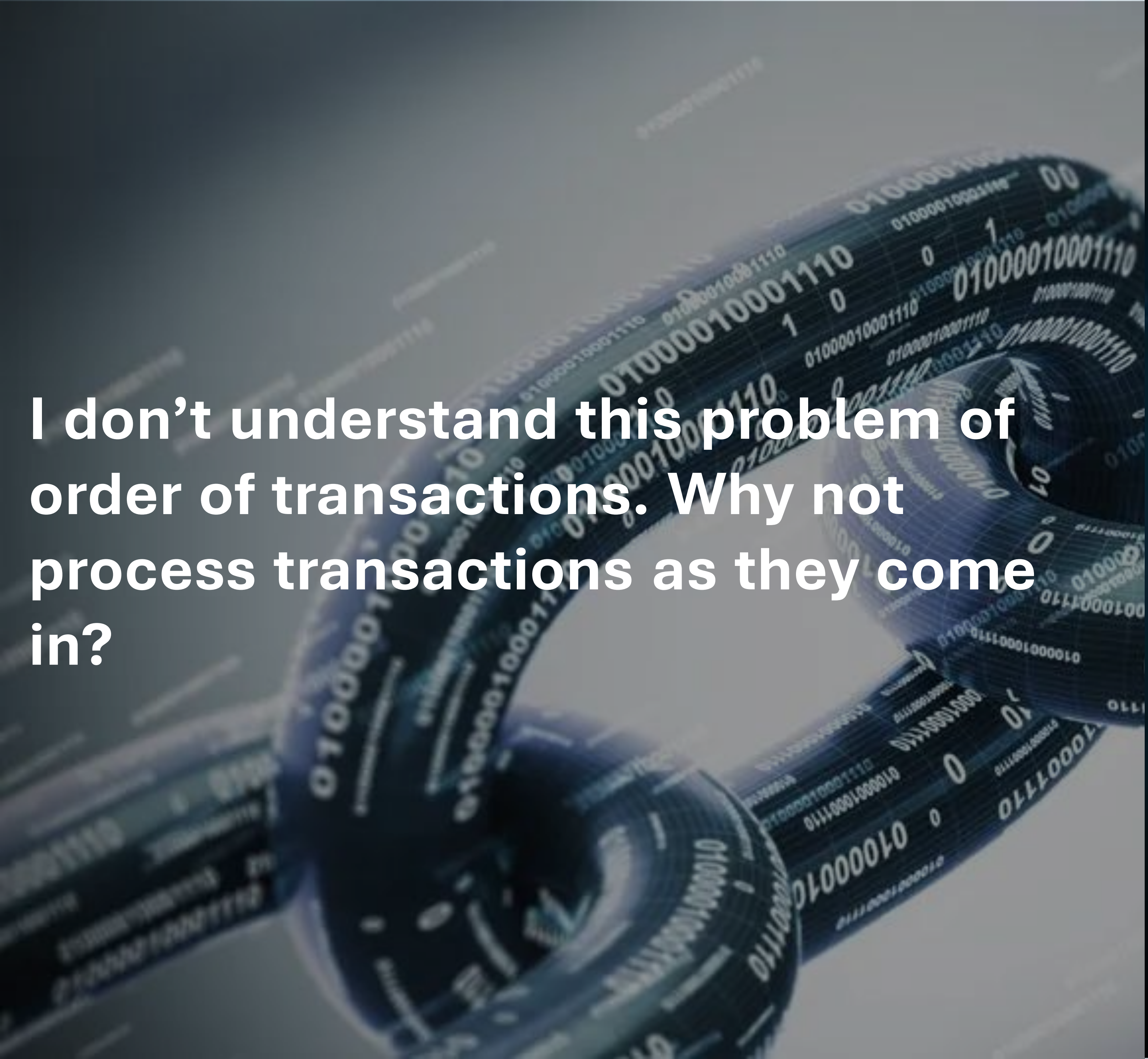
BRICK 4 – DETERMINISM





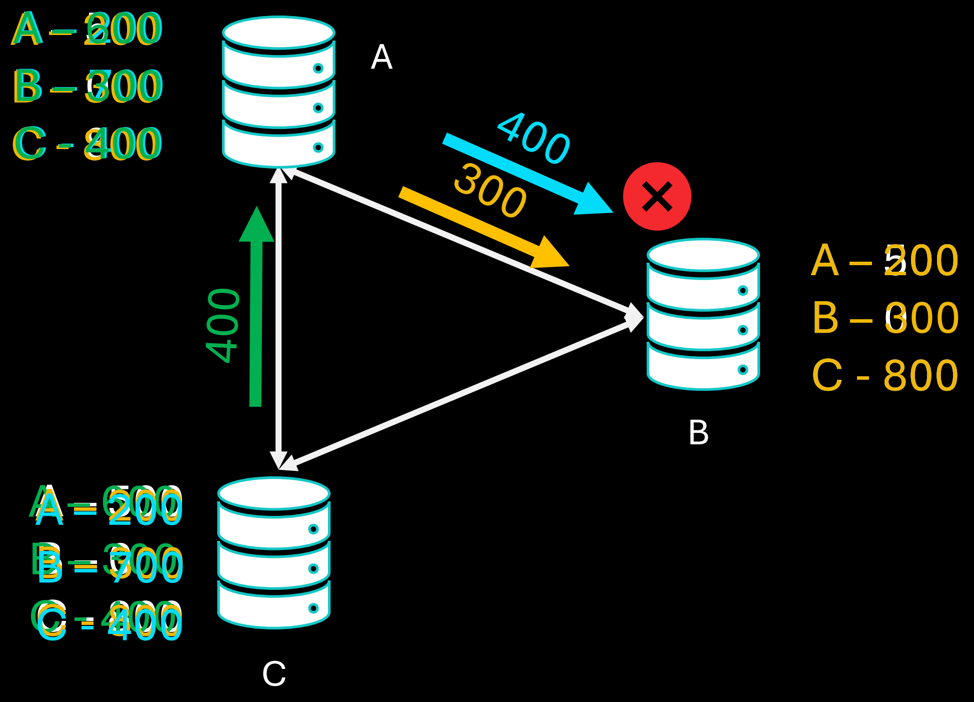
The term Determinism in Computer Science refers to a system where the future state of the system is entirely determined by the prior state and the current operation.

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.



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

BRICK 5 – ORDERING

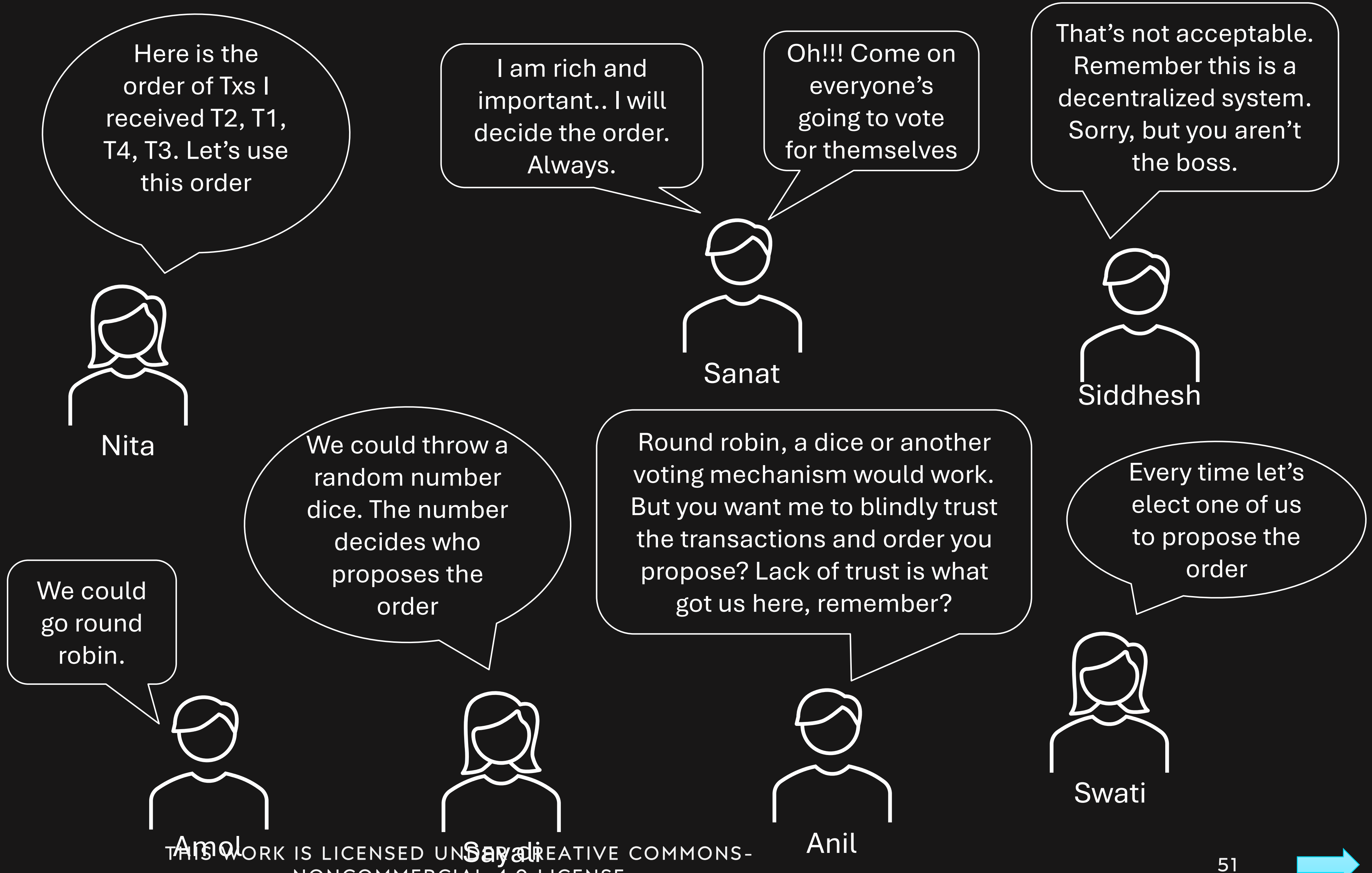


Who is right and who is wrong?

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

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

AN ORDERING CONUNDRUM



Here is the order of Txs I received T2, T1, T4, T3. Let's use this order

Nita

I am rich and important.. I will decide the order. Always.

Oh!!! Come on everyone's going to vote for themselves

Sanat

That's not acceptable. Remember this is a decentralized system. Sorry, but you aren't the boss.

Siddhesh

We could go round robin.

Amol

We could throw a random number dice. The number decides who proposes the order

Sayali

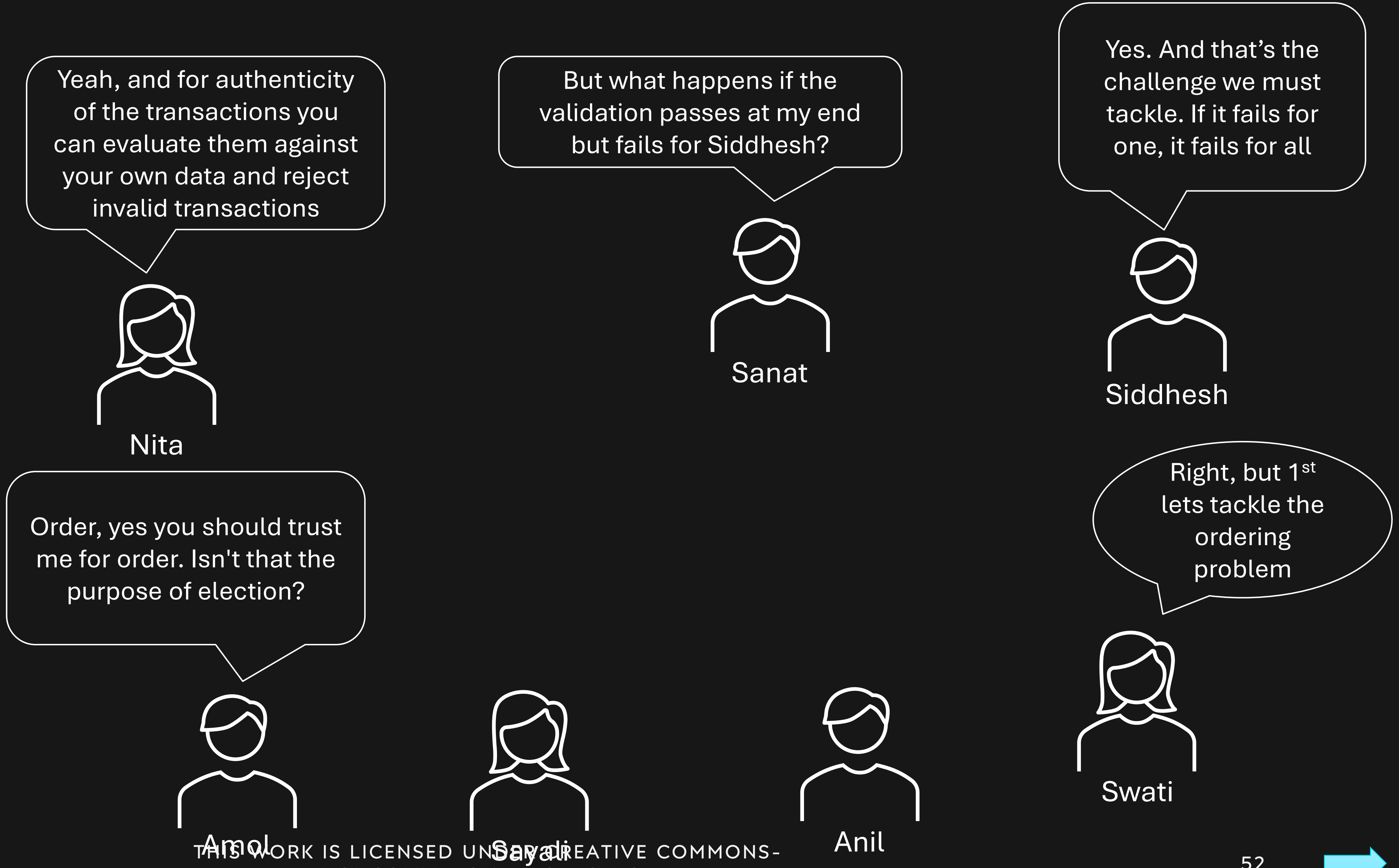
Round robin, a dice or another voting mechanism would work. But you want me to blindly trust the transactions and order you propose? Lack of trust is what got us here, remember?

Anil

Every time let's elect one of us to propose the order

Swati

AN ORDERING CONUNDRUM



Nita: Yeah, and for authenticity of the transactions you can evaluate them against your own data and reject invalid transactions

Sanat: But what happens if the validation passes at my end but fails for Siddhesh?

Siddhesh: Yes. And that’s the challenge we must tackle. If it fails for one, it fails for all

Amol: Order, yes you should trust me for order. Isn't that the purpose of election?

Swati: Right, but 1st lets tackle the ordering problem

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.

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

- 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