

Consensus

This is a class exercise where participants learn firsthand how difficult synchronizing actions is in a group without a defined leader. The intent is for participants to understand how agreement (i.e., consensus) is achieved in Bitcoin. In this activity you are going to facilitate three scenarios. In the first scenario, students track a simple set of transactions between three people. An analogy is friends lending each other money. It is simple enough that many will be able to do it without pen and paper. The second scenario involves seven entities (a bank plus six people). ONE student is designated as the official tracker for the whole class. The third and last scenario repeats the prior one with an important change: this time, ALL students track. No one can do any special favors (e.g., the banker cannot help his friend). This sets up the transition to discuss Bitcoin. Everyone can track the Bitcoin ledger for themselves, yet we are able to reach agreement (consensus) without a banker or other centralized tracker.

 ACTIVITY TYPE Game · Simulation	 DURATION 45 min	 PARTICIPATION Whole class · Individual
--	--	---

MATERIALS

- Something for all students to use to track, e.g., blank paper and pens
- Calculators for students are helpful, but not required
- For online classes, students can use spreadsheets

PREPARATION NOTES

Preparation time: 45 minutes.

Read through the steps in this guide a few times. Familiarize yourself with how each step builds upon the previous one. You will start simple and gradually work towards Bitcoin consensus.

Practice doing the math as if you were the student. This is very important. This preparation will ensure your class runs smoothly.

Class time: 45 minutes.

This activity has multiple rounds, each with multiple steps.

Expect clarification questions from students. Allow for time to address these questions.

Allow time for students to do the math calculations, especially if they are doing them by hand.

SETUP

There is very little set up needed. Distributing paper, pens, and calculators before class will speed up the activity.

Have your whiteboard or spreadsheet display ready before class as well. For example, draw the tracking tables before class. This will save time during the activity.

PROCEDURE

Step 1: Memory Only

Ask students to pick a fun medium of exchange other than bitcoin. Examples include dollars, monopoly money, pieces of candy, rocks, sheep, anything.

Since no physical items are necessary for this exercise, it does not matter what they choose. Explain to the class that you, the teacher, will be the guide for this exercise. Designate two students (or tables of students) to represent RED and BLUE.

Challenge students to track who has what using only memory if they can. Using pen and paper is fine as well. Give them time between steps to talk with one another.

- #1 – The TEACHER has 21 widgets, coins or whatever medium of exchange the students picked, and RED and BLUE have none
- #2 – TEACHER pays 2 widgets to RED
- #3 – TEACHER pays 5 widgets to BLUE
- #4 – BLUE pays 1 widget to RED
- #5 – TEACHER pays 5 widgets to RED

Ask how much the TEACHER has, how much RED has, and how much BLUE has.

Show or draw this table to clarify:

		TEACHER	RED	BLUE
STEP 1	TEACHER starts with 21	21	0	0
STEP 2	TEACHER pays 2 to RED	19	2	0
STEP 3	TEACHER pays 5 to BLUE	14	2	5
STEP 4	BLUE pays 1 to RED	14	3	4
STEP 5	TEACHER pays 5 to RED	9	9	4

The correct answers are 9 for TEACHER, 9 for RED, 4 for BLUE.

Step 2: Single-Ledger Tracker

Tell the students there will now be six colors and a bank. You, the teacher, will be the bank and you virtually distribute the money. **For this example, we are using 100 Monopoly money.** Explain that the class will have one designated student as the official tracker.

- #1 – The BANKER has 2,100 Monopoly dollars
- #2 – The BANKER pays each player 200 (ask the student who is the designated tracker to update the ledger, and to update the class on how much the teacher/bank now has (900).
- #3 – BLUE pays GREEN 200 (ask the designated student tracker to give a new summary of who has how much)
- #4 – BANKER pays ORANGE 800 (designated student tracker gives update)

		BANKER	RED	BLUE	PURPLE	BLACK	ORANGE	GREEN
STEP 1	BANKER starts with 2,100	2,100	0	0	0	0	0	0
STEP 2	BANKER pays each color 200	900	200	200	200	200	200	200
STEP 3	BLUE pays GREEN 200	900	200	0	200	200	200	400
STEP 4	BANKER pays ORANGE 800	100	200	0	200	200	1,000	400

- #5 – Tell the class that BLUE landed on a hotel on Broadway and needs 600 to pay GREEN. Ask if the bank (aka teacher) has enough?
- #6 – Explain that because **you, the teacher, are the banker you can create money.** You decide that you like BLUE. He is a friend of yours and you do not want him to go bankrupt so you create 600 from nowhere.

- #7 – You then give your friend BLUE 600

		BANKER	RED	BLUE	PURPLE	BLACK	ORANGE	GREEN
STEP 5	BLUE needs 600 to pay GREEN for his hotel on Broadway	100	200	0	200	200	1,000	400
STEP 6	BANKER declares it has printed 600 more dollars from nowhere	700	200	0	200	200	1,000	400
STEP 7	BANKER pays its friend, BLUE, 600	100	200	600	200	200	1,000	400

Step 3: Make the Bad Banker Stop

Inform the class you are repeating the exact exercise with one major difference. This time, instead of having one tracker, every student uses their own tracking sheet.

ALL students fill create and update a table.

After each step, ask if everyone agrees on who has how much.

At the point where the BANKER does not have enough money to help their friend BLUE, how many students agree?

In Step #2, agreement in the class (aka consensus) was dependent upon one person, the bank. In Step #3, agreement really is a consensus.

Explain that with Bitcoin, everyone has their own ledger.

There are thousands of NODE RUNNERS, people who run Bitcoin on their own computers and keep their own copy of the ledger, also called the blockchain. Instead of one central bank keeping track, it is tens of thousands of Bitcoiners keeping the decentralized ledger in sync.

CONSENSUS means the network agrees the protocol was followed correctly and disregards transactions that do not follow the protocol, such as the creation of extra bitcoin the BANKER did in this classroom example.

KEY POINTS

1. **Consensus = agreement**
2. One big difference between a group with centralized control and one without is the question of trust. Decentralized groups like peer-to-peer networks do not have a leader and participants do not trust each other. They require a different way to coordinate.
3. For developers of peer-to-peer networks, this is known as the Byzantine Generals Problem. Bitcoin solves this challenge with math and proof-of-work mining.
4. Bitcoin being decentralized is critical to its value. Historically, human leaders always succumb to the temptation to debase money over the long term.
5. The Nakamoto Consensus is named after the creator of Bitcoin, Satoshi Nakamoto. This consensus mechanism is how thousands of strangers who do not trust each other have maintained the Bitcoin ledger since 2009.

DISCUSSION QUESTIONS

Now that we have discussed Bitcoin in greater detail, let's look at our money comparison table from Chapter 2 again and see how bitcoin compares with other forms of money:

Characteristic of Good Money	Cows	Hot sauce	Diamonds	Paper Money	Bitcoin
Durable					
Portable					
Uniform					
Acceptable					
Scarce					
Divisible					
Total					

Guide the class to scarcity if they struggle. If central planners can help their buddies through money printing, money is not scarce.

ADDITIONAL RESOURCES

- [Video](#)

<https://youtube.com/watch?v=nS9LH5gu65Y&feature=youtu.be>

"Byzantine Generals Problem – Bitcoin" is a video produced by Jason Trio @bittrio. It simplifies the programming consensus challenge in a short story format.

- [Book](#)

<https://www.inventingbitcoin.com>

"Inventing Bitcoin: The Technology Behind the First Truly Scarce and Decentralized Money Revealed" by Yan Pritzker provides a high-level overview of Bitcoin's inner workings, including how consensus achieves scarcity.

- **A •** [Activity sheet \(designed handout\)](#)

<https://qr.myfirstbitcoin.org/consensus.pdf>