

Transactions in Action

This is a cooperative exercise simplifying the basic roles of people involved in a Bitcoin transaction: sender, recipient, miner, and node operator. In this activity you are going to facilitate transaction scenarios, for example "ALICE SENDS 1 BITCOIN TO BOB". Wallet addresses are simplified to just colors. Sats are simplified to just chips or coins. You will walk the class through a couple of scenarios where everything works well. The sender has enough sats. The sender has approved (signed) the transaction. Then you will walk through different ways transactions are not valid: not enough sats, transaction not signed, invalid wallet. The key point is that you cannot cheat Bitcoin because the ledger is protected by a network of miners and node runners. TIP: You can simplify the activity further by just having node runners if explaining the difference between miners and node runners distracts from the main point of the activity, transactions in action. TIP: Depending on the age and knowledge level of your class, consider rotating students through the different roles.

ACTIVITY TYPE Game · Role-play	DURATION 30 min	PARTICIPATION Whole class
---	----------------------------------	--

MATERIALS

- This activity can be done with just a whiteboard or a spreadsheet projected on a screen. With this method, there are no additional materials needed.
- This activity can also be done with physical items which may be more impactful for younger audiences.
- Color paper (4 to 6 colors) (representing wallets)
- 21 poker chips, coins, or other material (representing sats)
- Whiteboard or projector screen (for tracking transactions)

PREPARATION NOTES

Preparation time: 15 minutes.

The hardest part of preparing for this activity is reviewing the transaction scenarios a few times.

Consider adjusting the amounts and the stories to fit your audience. Consider making it more fun by using competitive sport mascots instead of colors.

Class time: 30 minutes.

Expect students to grasp the tracking system quickly, but repetition will be helpful to increase their understanding of Bitcoin transaction mechanics. Repeat the conditions necessary for a valid transaction. Repeat, then repeat, then repeat them again.

Pause to allow time for questions and discussion.

SETUP

Set up is simple. To save time, draw the tracking table on your whiteboard or create it in your spreadsheet before class starts.

Sats	Red	Blue	Green	Orange	Total
Starting	12	4	7	2	21
Round 1					
Round 2					
Round 3					
Round 4					
Round 5					

The amounts in this table, and in the tables in each step below, are the example values the activity sheet uses.

If you are using the physical representations of the wallets (paper) and sats (poker chips or coins), gather these materials before class.

PROCEDURE

Step 1: The First Transaction

Guide students through to the tracking board. Assign four students to be the owners of each of the four-colored wallets. Explain their responsibility is to sign or not sign (approve, not approve) transactions.

If you are using the physical method, hand out their respective color "wallets" (papers). Also give them the corresponding number of poker chips (or coins, or whatever you have decided to use for sats).

Explain to the rest of the class they each represent miners or node runners. Their responsibility is to agree or not agree whether a transaction is valid. They decide to accept or reject transactions. For the game, select one of them to be responsible for updating the tracking board.

Now walk the class through the first transaction step by step. Tell them a story of how RED bought a coffee from BLUE for 5 sats.

Ask "RED, do you agree to pay 5 sats to BLUE?"

Keep narrating. Your goal is to get RED to agree to send money to BLUE. When they do agree, tell them to say the following out loud: "I, RED, sign this transaction."

"NODES and MINERS, is the transaction RED SENDS 5 SATS TO BLUE valid?"

1. Does RED have 5 sats?
2. Did RED sign the transaction?

If both conditions are met, instruct the tracker to update the table. Ensure they update the total column too. This will always be 21.

If you are using the physical method, ask one of the miners to move 5 sats (chips) from the red wallet (paper) to the blue wallet (paper).

Sats	Red	Blue	Green	Orange	Total
Starting	12	4	7	2	21
Round 1	7	9	7	2	21
Round 2					
Round 3					
Round 4					
Round 5					

Step 2: The Second Transaction

Continue narrating. This time BLUE is buying something (perhaps a book) from ORANGE for 7 sats.

Walk the class through the steps like before.

"BLUE, do you agree to pay 7 sats to ORANGE?"

"NODES and MINERS, is the transaction BLUE SENDS 7 SATS TO ORANGE valid?"

1. Does BLUE have 7 sats?
2. Did BLUE sign the transaction?

If both conditions are met, instruct the tracker to update the table. Ensure they update the total column too.

If you are using the physical method, one of the miners moves 7 sats (chips) from the blue wallet (paper) to the orange wallet (paper).

Sats	Red	Blue	Green	Orange	Total
Starting	12	4	7	2	21
Round 1	7	9	7	2	21
Round 2	7	2	7	9	21
Round 3					
Round 4					
Round 5					

Step 3: Not Enough Sats

Continue narrating. This time GREEN is buying something (perhaps a meal) from RED for 10 sats.

Walk the class through the steps like before.

"GREEN, do you agree to pay 10 sats to RED?"

"NODES and MINERS, is the transaction GREEN SENDS 10 SATS TO RED valid?"

1. Does GREEN have 10 sats?
2. Did GREEN sign the transaction?

The node runners and miners should NOT agree the transaction is valid because GREEN does not have enough sats.

"NODES and MINERS, will you process this transaction?"

When they say "no", instruct the tracker to update Round 3 with no changes from Round 2.

Sats	Red	Blue	Green	Orange	Total
Starting	12	4	7	2	21
Round 1	7	9	7	2	21
Round 2	7	2	7	9	21
Round 3	7	2	7	9	21
Round 4					
Round 5					

Step 4: Transaction Not Signed

Continue narrating. This time, there is no purchasing story. ORANGE is trying to get GREEN to send him 5 sats.

"GREEN, do you agree to pay 5 sats to ORANGE?"

GREEN should say "no".

"NODES and MINERS, is the transaction GREEN SENDS 5 SATS TO ORANGE valid?"

1. Does GREEN have 5 sats?
2. Did GREEN sign the transaction?

The node runners and miners should NOT agree the transaction is valid because GREEN never signed (approved) it.

"NODES and MINERS, will you process this transaction?"

When they say "no", instruct the tracker to update Round 4 with no changes from Round 3.

Sats	Red	Blue	Green	Orange	Total
Starting	12	4	7	2	21
Round 1	7	9	7	2	21
Round 2	7	2	7	9	21
Round 3	7	2	7	9	21
Round 4	7	2	7	9	21
Round 5					

Step 5: Invalid Wallet

Continue narrating. ORANGE is still being sneaky. If he cannot get sats from another wallet, perhaps he can trick the network into updating his wallet with fictional sats.

Tell the class that ORANGE broadcasts the following transaction to the network, "PURPLE SENDS 4 SATS TO ORANGE".

"NODES and MINERS, is the transaction valid?"

No one can create sats from nothing. They must come from an existing and valid wallet.

The node runners and miners should NOT agree the transaction is valid because PURPLE is not a real wallet.

"NODES and MINERS, will you process this transaction?"

When they say "no", instruct the tracker to update Round 5 with no changes from Round 4.

Sats	Red	Blue	Green	Orange	Total
Starting	12	4	7	2	21
Round 1	7	9	7	2	21
Round 2	7	2	7	9	21
Round 3	7	2	7	9	21
Round 4	7	2	7	9	21
Round 5	7	2	7	9	21

KEY POINTS

1. There are four types of participants in every Bitcoin transaction: the sender, the recipient, miners, and node operators.
2. The sender must approve (cryptographically sign) the **amount of bitcoin** to send AND the **specific address** to send to.
3. The recipient must provide a **valid address** to the sender AND verify the transaction was successfully confirmed on the blockchain.
4. Miners ensure all criteria are valid before adding transactions to future blocks.
5. Node operators verify mined blocks are valid before updating their version of the blockchain (the ledger).

DISCUSSION QUESTIONS

- Why is it important to have many people watching and validating transactions?
- Is there a way to double-spend sats by broadcasting two transactions simultaneously?
- Did everyone notice how the total number of sats never changed?
- How is this different than the fractional banking activity?
- Why does Bitcoin use cryptography to sign transactions?

NOTES

Rotate through all four roles to experience what each participant does.

ADDITIONAL RESOURCES

- [Video](https://blockchain.mit.edu/how-blockchain-works)
<https://blockchain.mit.edu/how-blockchain-works>
"Blockchain 101 - A Visual Demo" by Anders Brownworth and posted through MIT. <https://blockchain.mit.edu/how-blockchain-works>
- [Book](https://www.inventingbitcoin.com)
<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. <https://www.inventingbitcoin.com>
- **A** • [Activity sheet \(designed handout\)](https://qr.myfirstbitcoin.org/transactions.pdf)
<https://qr.myfirstbitcoin.org/transactions.pdf>