How does Bitcoin work?

Pavel Kravchenko

Challenges for decentralized electronic money creation

How to remove the need of central organization and trust to one party?

How to ensure honest voting process in anonymous, trustless, decentralized system?

How to prevent double-spending?

How to encourage users to join the system?

Principles of Bitcoin

Each participant stores all transactions in the system at their own database

Order of transactions in this database is fixed

Adding new transaction to the chain requires verification and execution of some hard work

Everybody should do transaction verification – which is the key to system's stability

Transactions are verified every 10 minutes, only one participant becomes the first to do that

New coins appear in the system as reward for transaction verification

Principles of Bitcoin

Code of Bitcoin is open source

Only owner of the private key can spend funds

All decisions are made by simple majority

Fees are taken by participants and set on their own decision

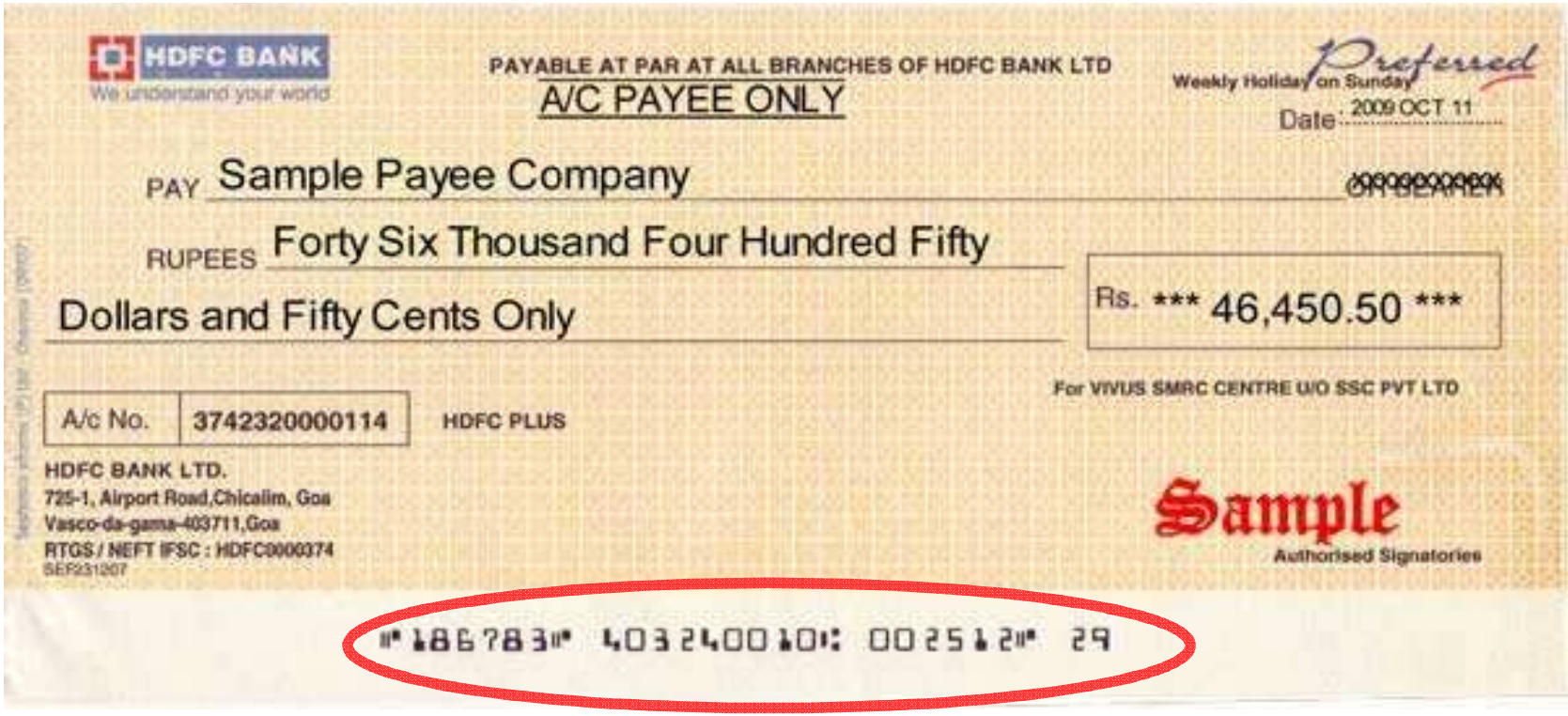
Now we will pass 7 steps towards imaginary cryptocurrency creation, during which we will cover possible attacks and their preventions

Step 1. The simplest e-money

Digital receipt signed by the private key of the user

Step 2. How to distinguish copy from original?

To distinguish copies of the same cheque we introduce ***unique receipt identifier***



Step 3. Verification of the incoming cheque

Everybody can verify unique identifier in their own copy of the database (blockchain).

Step 4. How to verify that incoming cheque was not spent before?

You have to ask other participants – each of them provides a vote

Most important questions

How many participants have to vote to accept or reject particular transaction?

How can you define “participant”? Is it a person or a piece of code?

How many participants take part in the voting process?

Do they know and trust each other? Probably not.

How to ensure honest voting process in such conditions?

Step 5. How to prevent buying votes

To vote you have to present proof-of-work

Only the first vote is counted

There is a reward for being the first

How does “hard task” should look like?

Everybody has a chance to win

It should be able to prevent fraud

Everybody can verify results

The result of one participant cannot be stolen by another

It should encourage participants to work more

The closest analogue of such a task is participation in the lottery – everybody has a chance to win, but those who buy more will more likely win.

Mining in Bitcoin it is just a process of permanent checking answers for certain mathematical equation. It is not connected to transaction verification – it is just needed to prevent votes “buying”.

Step 6. Everybody competes to win

Probability of being the first is equal to percentage of computational power that you have

You can control the network if you have 51%+ computational resources

System is trustworthy until honest participants control 51% of power

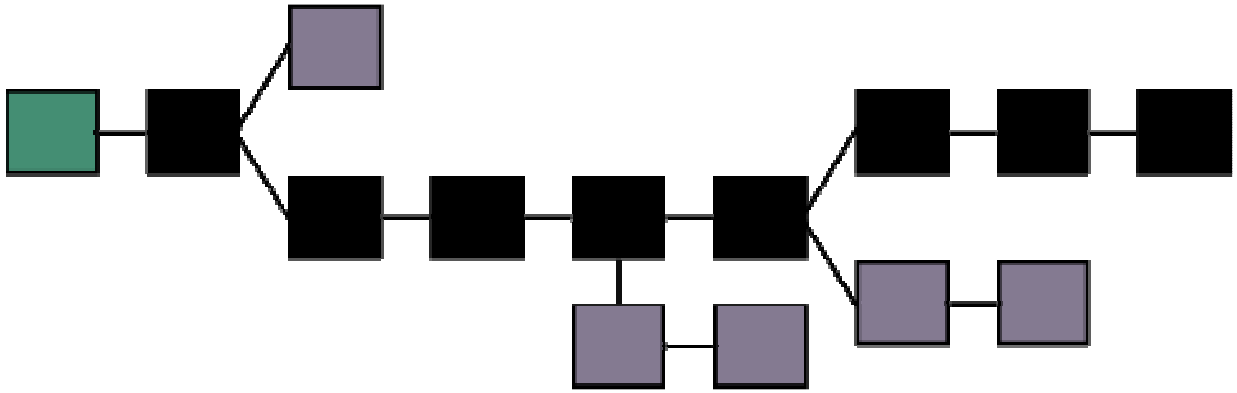
Doesn't matter who out of **honest** participants will win

The fastest supercomputer in the world cannot even control 0.01% of power needed to control the system

It looks like brain-ring game – everybody wants to submit the answer (in our case after solving “hard task”) - but only the first gets the right to tell the answer

Step 7. How to define who was the first?

1. There are delays and attacks in the network
2. If fork occurred, both chains are saved
3. Each block (set of confirmed transactions) contains pointer on the previous one
4. Work continues in the longest chain
5. Transaction is fully confirmed if it is in the longest chain and there are 5 confirmed blocks after



Drawbacks of Bitcoin

Low performance (3-7 transaction per second)

A big amount of data to store (currently ~30GB)

Traceability of transactions (database is public)

Electricity consumption by miners (~$0.5M / day)