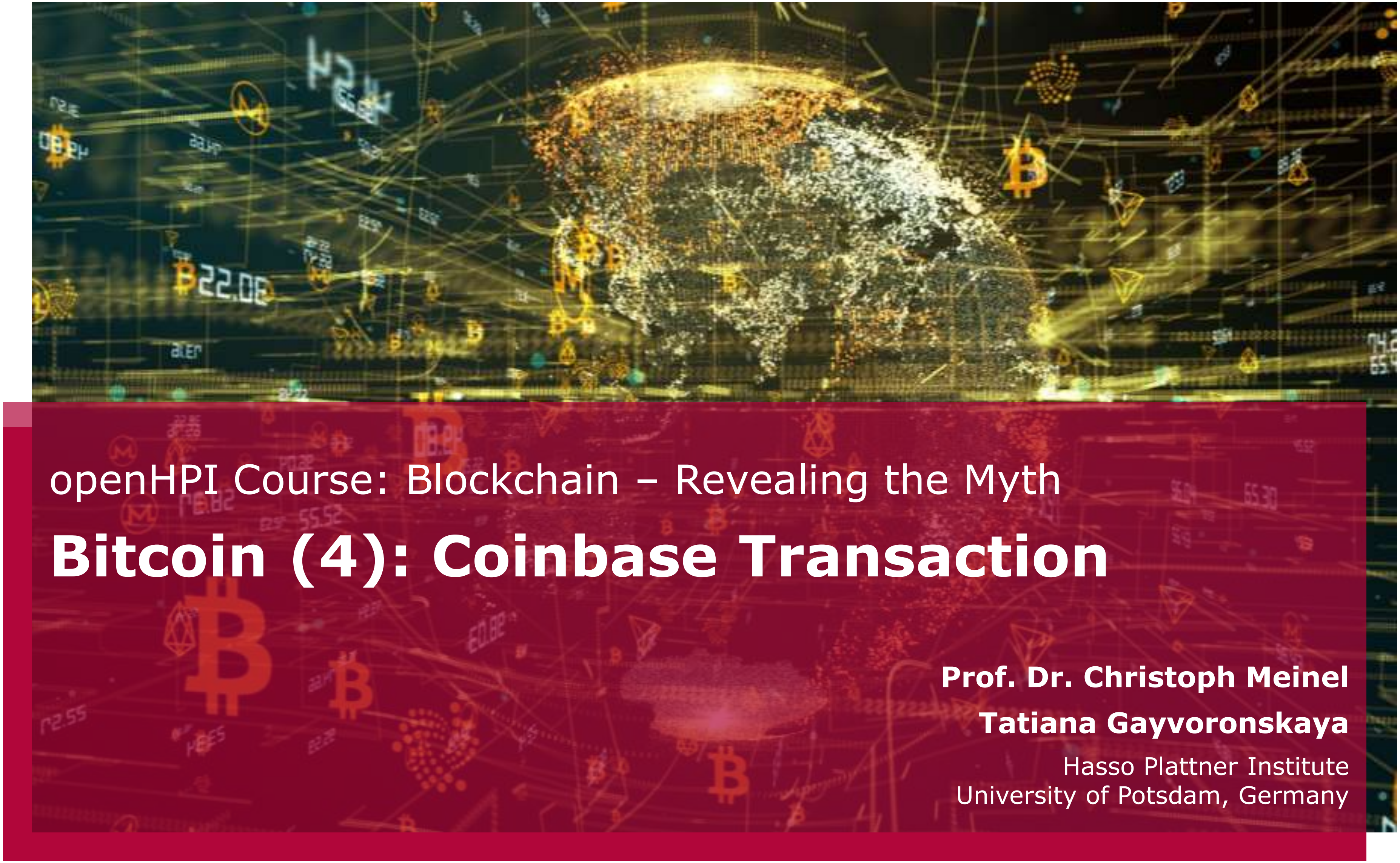


openHPI Course: Blockchain – Revealing the Myth

Bitcoin (4): Coinbase Transaction

Prof. Dr. Christoph Meinel

Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

Blockchain – Incentivize Users

Step by step, we realize **how complex** the Bitcoin solution is for a system for electronic transactions that do not rely on trust

Review:

- We have a system for participants to agree on a single chronological order of transactions
- The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it
- We have a solution to the double-spending problem using a peer-to-peer distributed timestamping to generate computational proof of the chronological order of transactions

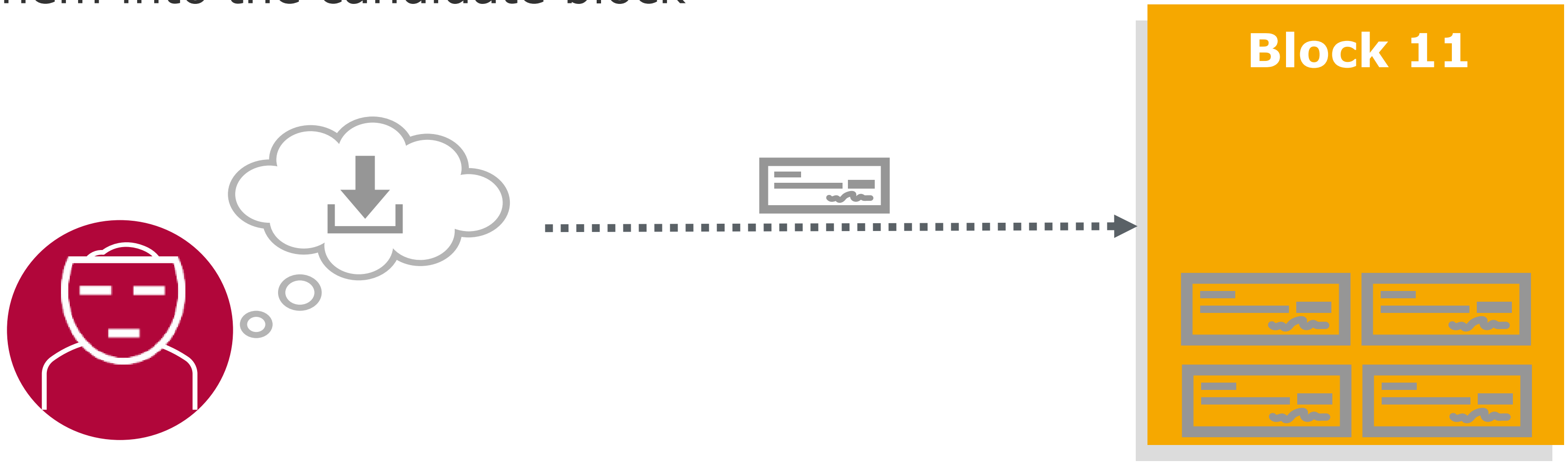
Central Question: **How users are incentivized**

- to **comply with the rules** and
- to **provide a proof-of-work**?

Creating New Blocks – Mining New Coins (1/3)

In the last video clip we indicated that **new coins** are **“mined” by the work done**

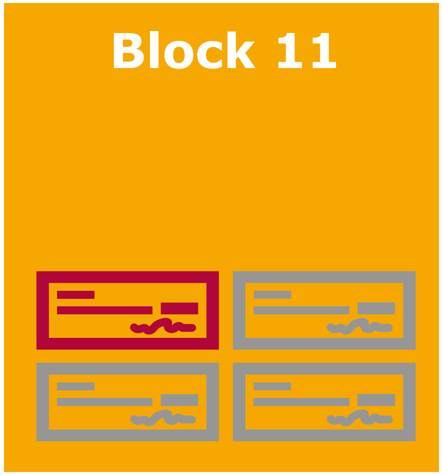
- So, if a user has decided to **participate in the race** and try his luck to get the **reward** for a successful generated block, then he starts to create a new block, a so-called **candidate block**
- To this end, the user takes out all transactions from his **memory pool** – a **buffer** he has stored all received transactions – and fills them into the candidate block



Creating New Blocks – Mining New Coins (2/3)

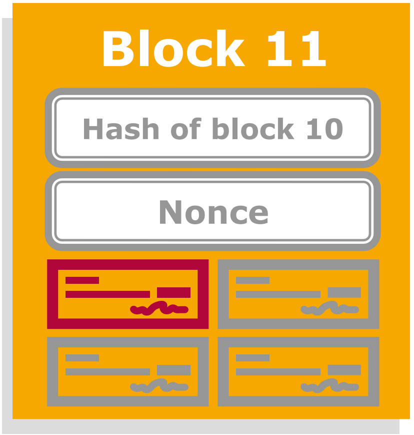
The **first transaction** in a block is a special transaction that starts a **new coin** owned by the user who creates the block

- This transaction is also called a **coinbase transaction** and it allows the user to **send himself a fixed amount** of coins that did not previously exist together with the **fees for the transactions** included in the block
- After 210,000 blocks, **the rewards** paid to the miners in form of newly created coins **will be halved**
  - □ approximately every 4 years, e.g.
    - – starting in 2020 there are only 6.25 bitcoin



Creating New Blocks – Mining New Coins (3/3)

- Creation of a new block **generates a hash of the previous block** and adds it to the block
- Then he generates a **hash of the block** in combination with a **nonce** and hopes that it is below the current target
- As soon as he has found an **appropriate nonce** he can **broadcasts** the created block **to the network**



Coins of the Coinbase Transaction

- The user would be able to **spend the coins** he claimed from the **coinbase transaction** once the block becomes at least **99 successor blocks** in the **longest chain**
- Therefore, this block reward acts as an incentive for miners to mine new blocks and **continually try to extend the longest known chain** of blocks
- Last but not least, we would like to have a closer look at the **structure and content of the transaction**

Summary

- The **first transaction** in a block is a special transaction that starts a **new coin** owned by the user who creates the block, so called a **coinbase transaction**
- This transaction allows user to send himself a reward in form of fixed amount of coins that did not previously exist together with the **fees for the transactions** included in the block