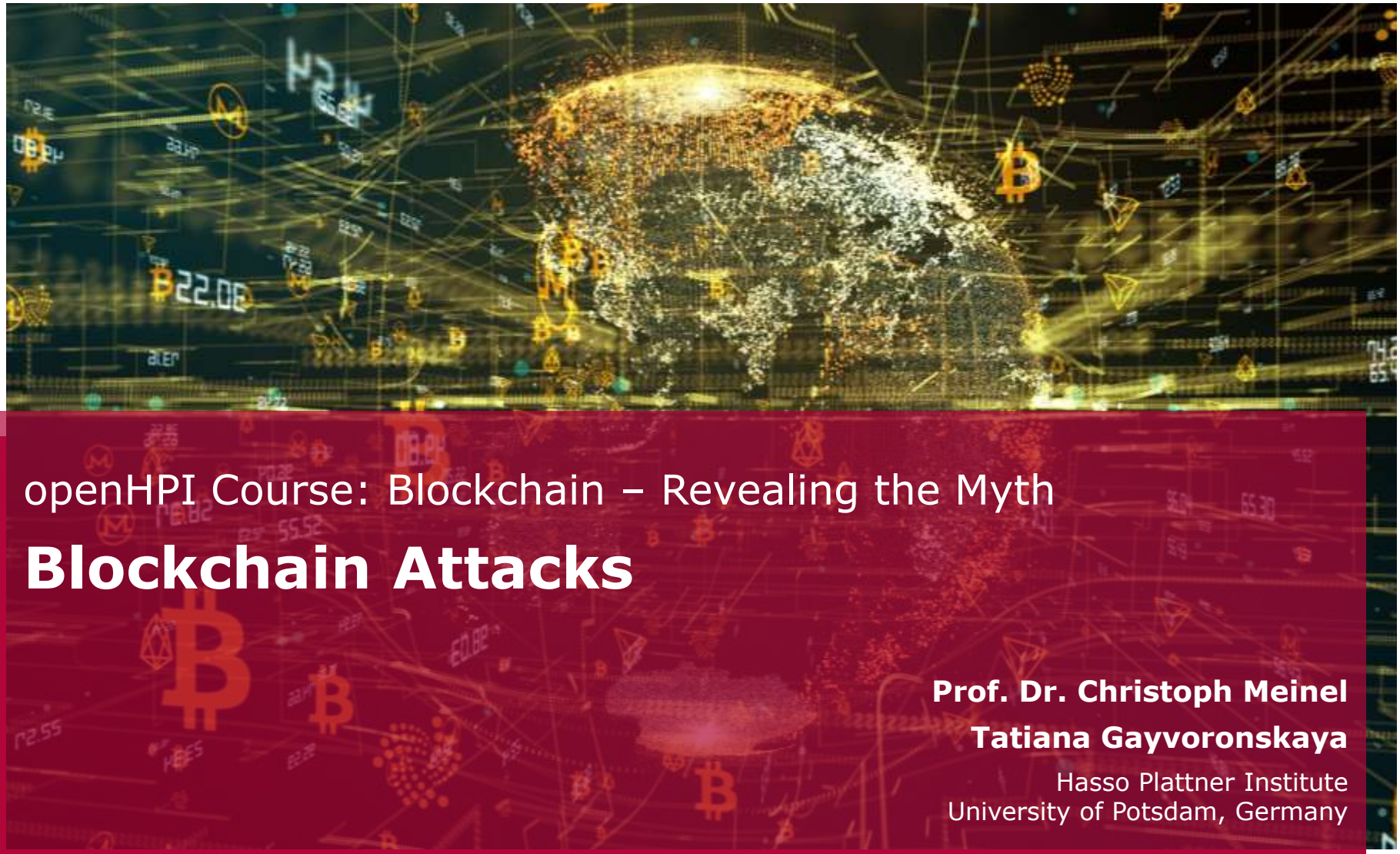


openHPI Course: Blockchain – Revealing the Myth

Blockchain Attacks

Prof. Dr. Christoph Meinel
Tatiana Gayvoronskaya
Hasso Plattner Institute
University of Potsdam, Germany

Security

We have considered the functionality of the Bitcoin system but **no IT-system is "unhackable"**

- Existing peer-to-peer application attacks have to be considered in blockchain-based systems too
- A number of blockchain specific attacks have been formalized
- We will look at some basic attacks
  - Eclipse attack
  - 51 percent attack

Security
Eclipse Attack

The attacker in a peer-to-peer network attempts to **monopolize the connections of the victim**

- Attackers attempt to be the only one connected to the victim
- Attackers then withhold or forward selected blocks and transactions, and in this way
  - **shut out the victim from the network**
  - **manipulate the victim's view of the blockchain**
- Bitcoin clients have connections initiated by themselves (**outgoing connections**) and connections requested by other users (**incoming connections**) to avoid this attack

Security
51 Percent Attack

If an attacker in a blockchain-based system has **more than 50 percent of the total resources of the system** (computing capacity or proportion of coins), the following manipulations of the blockchain are possible:

- **Monopolizing the mining** of new blocks, and thereby keeping the reward exclusively
- Asserting the **own blockchain** as the longest chain
- Only including **blocks of own transactions** or blocking transactions of certain users (not including them in the blocks)
- Carrying out **double-spending**

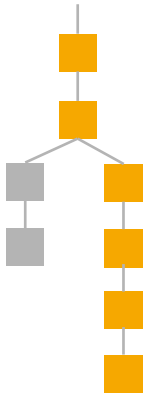
This procedure is also known as the **51 percent attack**

- **PoS is more vulnerable** to the 51 percent attack, as PoW (since in case of PoS loss is not as noticeable)

Security
Double Spending – Example (1/2)

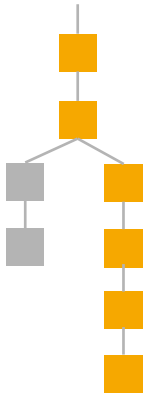
The attacker **re-uses** his **already issued values** multiple times

- Imagine that a **malicious user** has **bought** expensive photographic equipment for **half a Bitcoin**
- His transaction to the seller was recorded in **block number 700,000**
- After **six blocks** transaction confirmation time, the **seller** has **sent the goods** to the user
- **After receiving** the photo equipment **after a half day**, the malicious user **wants to get back** the money he spent
- He creates a **new transaction** in which he transfers **the half Bitcoin** already spent **to himself** (both transactions, old and new, have the same input)



Security
Double Spending – Example (2/2)

- This transaction goes into a **new block with the number 700,000**
- After a half day **72** (=12 x 6) **new blocks** have already been created following the earlier block 700,000
- He **cannot** simply **exchange the block**, because the new block has a completely different hash value
- This means, **all other 72 blocks have to be recalculated** because the entire **hash chain is no longer correct**
- But this is not enough, the malicious user must **enforce the new chain** until it is **longer than the other chain**
- Otherwise, it would look like **he never sent his money** to the seller of the photo equipment



Security

We have now looked at **two examples** of attacks on the blockchain

- They represent **two types of attacks**
  - Consensus algorithm attacks
  - Network attacks
- The most effective attacks will **combine these types**
- However, they are often times very **elaborate** and **difficult**
- The user often times is still the weakest part of the system
  - Tricking user to make wrong transaction
  - Stealing private key of users