openHPI Course: Blockchain – Revealing the Myth

Bitcoin (3): Incentives and Mining

Prof. Dr. Christoph Meinel

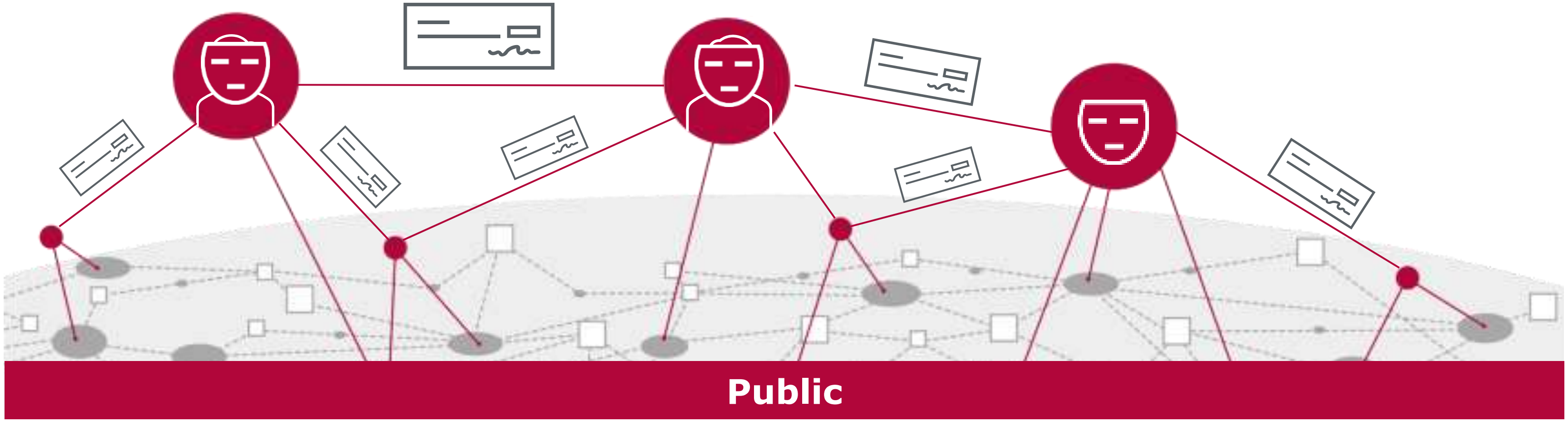
Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

Bitcoin Network

Review:

- So far, we know that we have a **peer-to-peer network** with **anonymous users** who **broadcast** all transactions (theirs and those they received from other users)



Bitcoin Network

Let's take a closer look on the **steps to run our network**:

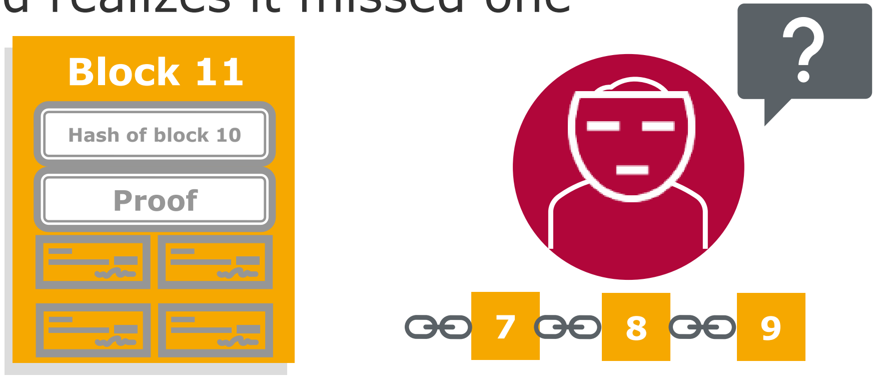
1. New transactions (new transactions created by the user and transactions received from others) are **broadcast** to all users
2. Each user **collects** new transactions **into a block**
3. Each user works on finding a **difficult proof-of-work for its block**
4. When a user finds a proof-of-work, it **broadcasts the block** to all users
5. …

Bitcoin Network

4. …
5. Users accept the block only if all transactions in it are **valid and not already spent**
6. Users express their **acceptance** of the block by working on creating the next block in the chain, using the **hash of the accepted block as the previous hash**
7. Users always consider **the longest chain** to be the **correct one** and will keep working on extending it

Bitcoin Network

- Messages (transactions and blocks) are broadcast on a **best effort basis**, and users can **leave and rejoin the network** at will, accepting the **longest proof-of-work chain** as proof of what happened while they were gone
- New transaction broadcasts **do not necessarily need to reach all users**
- As long as they **reach many users**, they **will get into a block** before long
- If a user does not receive a block, it will **request it when it receives the next block** and realizes it missed one

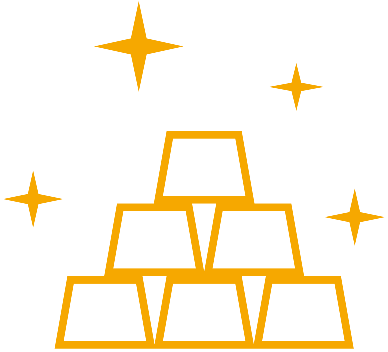


Bitcoin Network
Incentives for the User

- This **inspection** of our network has once again made us aware of the **absence** of the **central authority** and any **third party**
- Measures like proof-of-work against fraud are being taken, but **we still see no significant reason** so far **why** our users should want **to do such work**, which involves costs (consumption of electricity)
- Since we want to have an **electronic cash system** that is **independent of third parties**, we need still a **peer-to-peer mint** to issue the new currency

Bitcoin Network
Incentives by Newly Minted Coins (1/2)

- What is needed is to **reward users** for doing work (proof-of-work) **with newly minted "coins"**
- Such **incentives for users** that support the network provides a way to initially **distribute coins among users and bring them into circulation**
- The steady addition of a constant amount of new coins is analogous to **gold miners expending resources** to add new gold to circulation. In our case, it is **CPU time and electricity** that is expended
- The incentive can also be funded with **transaction fees**



Bitcoin Network
Incentives by Newly Minted Coins (2/2)

- Thus, the process of performing the proof-of-work and generating new coins is compared with that of **extracting raw materials**, and one speaks of **mining**
- Correspondingly, a user who performs a proof-of-work and creates new blocks is called a **miner**:
  - “whoever mines carries out hard work to get to the desired material”

Summary

A greedy attacker ought to find it **more profitable** to **play by the rules**, since

- the rules favor him while potentially bringing more new coins than everyone else and
- the rules stable the system and **validity of his own wealth**