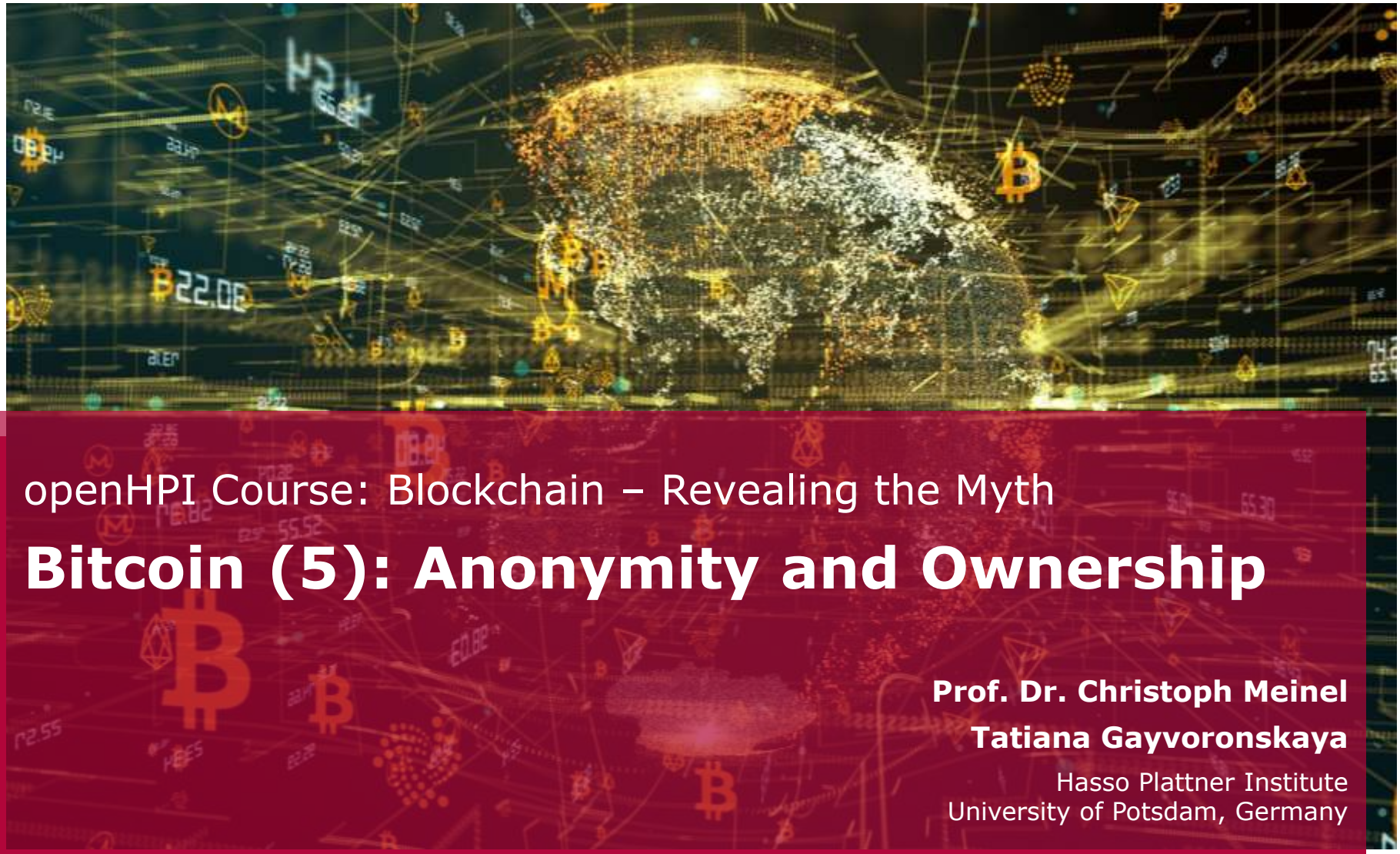


openHPI Course: Blockchain – Revealing the Myth

Bitcoin (5): Anonymity and Ownership

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

Transaction in a Standard Banking System

In a standard banking system, for example, a **transaction** is a requests to **move an amount of money** from one user account to another

- Assume **Alice transfers 2$ to Bob**:
  - it reduces the value in **Alice's account by 2$** and increases the value in **Bob's account by 2$**
  - if Alice's account has **less than 2$,** the system returns an error

Bitcoin transactions have a different structure

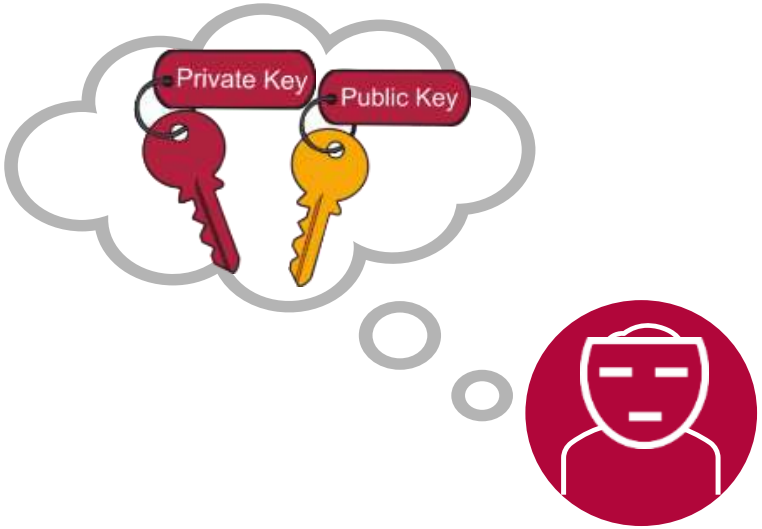
Alice	Bob
80$ - 2$	50$ + 2$

Anonymity of Bitcoin Users

In order to credit a user with a **Bitcoin value** (coin), **cryptographic methods** are used for

- **anonymizing user accounts**, so called **"addresses"**, and
- **creation of coins**

In both cases, methods from **public key cryptography** are used



Anonymous Addresses and Signed Transactions

Each user generates a cryptographic **key pair**

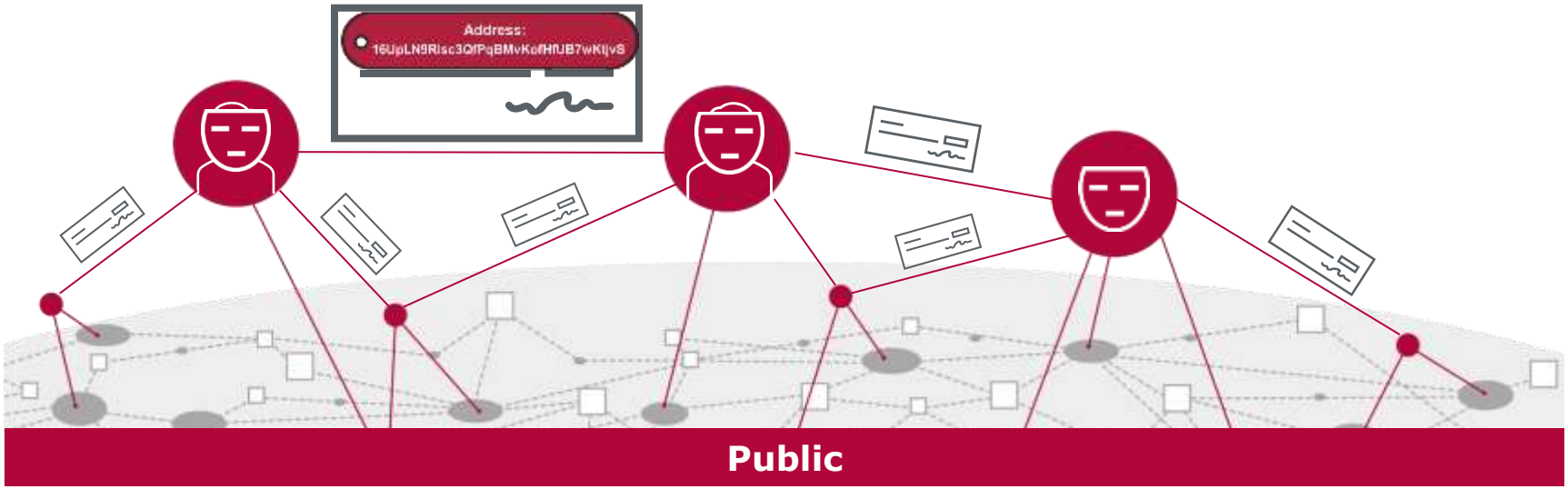
- **Private key** is used for **signing transactions** (confirmation of ownership)
- **Public key** is used for generating **addresses**

Anonymous Addresses: Hash of the User's Public Key

- First, the **private key** is generated, considered as random number
- The **public key** is derived from the private key and then **"hashed"**
- In the end, the **160-bit alphanumeric value,** e.g., *16UpLN9Risc3QfPqBMvKofHfUB7wKtjvS* is used as the **"address"**
- When a transaction is verified by an user, he checks, among other validity rules, **whether the transaction is addressed to his address**
- Hence, users do not need to be identified, since **transactions are not routed** to any particular node. They are only delivered on a best effort basis

Anonymous Addresses: Hash of the User's Public Key

- The public can "see" that **someone** is sending an amount **to someone** else, but has not **information about the user** who is linked to the **transaction**
- As an additional firewall, a **new key pair** could be used **for each transaction** to keep them from being linked to a common owner



Anonymous Addresses and Signed Transactions

Summary

- In order to credit a user with a **Bitcoin value** (coin), **cryptographic methods** are used exclusively in the **creation of coins** and **anonymous user addresses**
- The **private key** is used for **signing transactions** (confirmation of ownership) and the **public key** is used for generating **addresses**