openHPI Course: Blockchain – Revealing the Myth

Scalability: Off-Chain Approaches

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

Off-Chain Approach

Now let us consider other scaling options, so-called **off-chain transactions**:

- Transactions are **carried out outside of the blockchain** and thus they are not registered in the blockchain
- **But** the **security** of the system can be **compromised** because the transactions are no longer **verified in the network**
- Both **Bitcoin** and **Ethereum** are working on possible secure off-chain solutions:
  - micropayment channels
  - state channels
  - child chains
  - side chains

Payment and State Channels

Payment Channels

- Between users **temporary payment channels** are created
- As long as the **channel is open**, users can **exchange transactions** in **large numbers** and **high speed**
- After **expiration** of the agreed time, these transactions, or a **sum total transaction**, are **released** for the blockchain
- This allows a virtually **instantaneous**, **fee-free**, **scalable** and **confidential** exchange of values

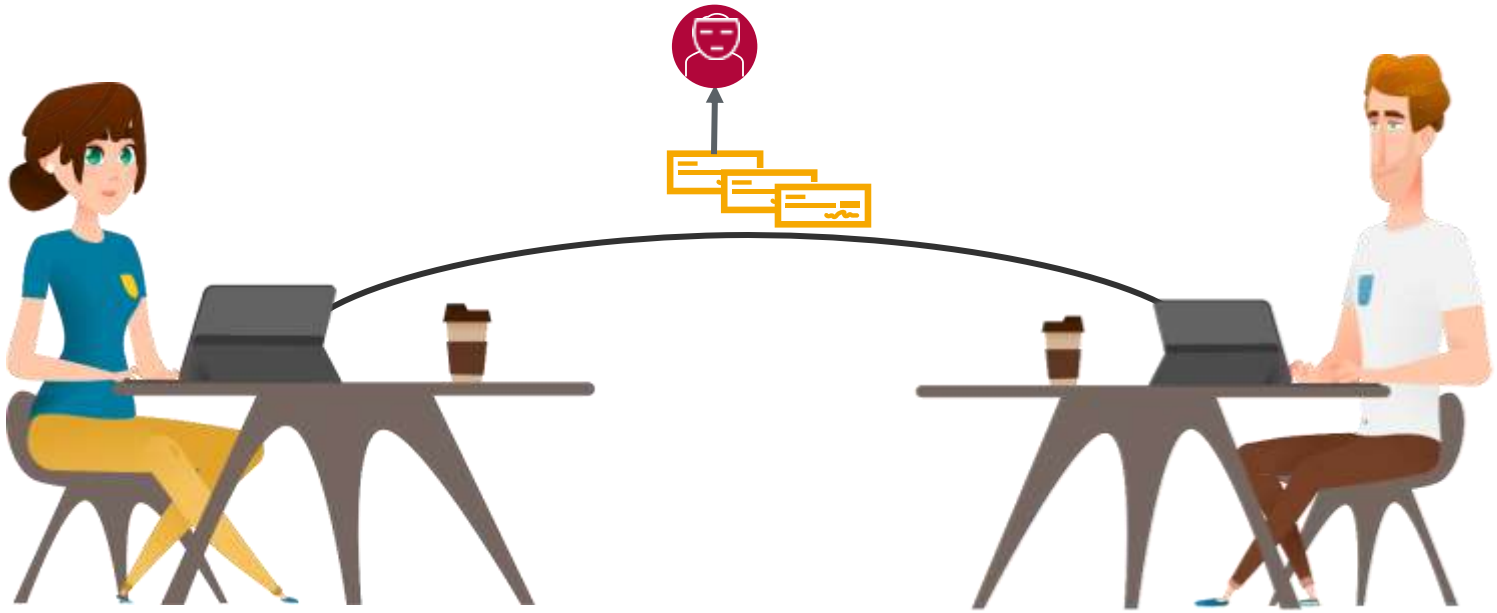
State Channels

- Another next off-chain solution similar to the payment channels are so-called **state channels**
- Here the **states are updated outside of the blockchain** instead of the values

Example of State Channels

Let us illustrate this by means of an **example**, a **chess game between Alice and Bob**

- Instead of sending a new transaction with the state update to the Ethereum network after every chess move states are updated in a state channel
- Then, only the last transaction is sent to the network



Summary

As we have already seen, with all **scaling options** **we are forced to make compromises** on the **decentralization** or the **security** of the system

- So, we find ourselves once again at the **scalability trilemma**
- With this in mind, we close this clip with the following thought:

*The focus of blockchain technology is a **robust** and **secure** **decentralized** system **without any conditions** for the number of system users or their identification. Yet in an attempt **to make** the blockchain **more efficient**, the **security** or the **decentralization** of the system often **suffers***