



openHPI Course: Blockchain – Revealing the Myth

Scalability Trilemma

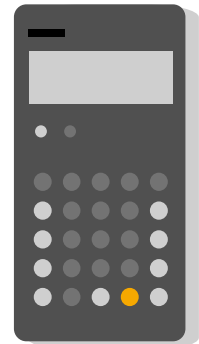
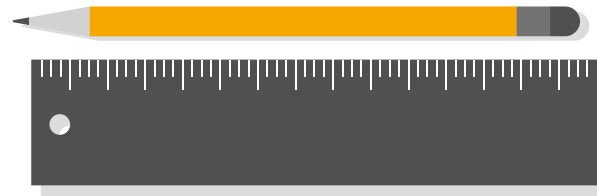
Prof. Dr. Christoph Meinel
Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

More Efficiency – Less Decentralization or Security

In an attempt to **make blockchain-based systems “more efficient,”** either the **decentralization** or the **security** of the system **gets lost**

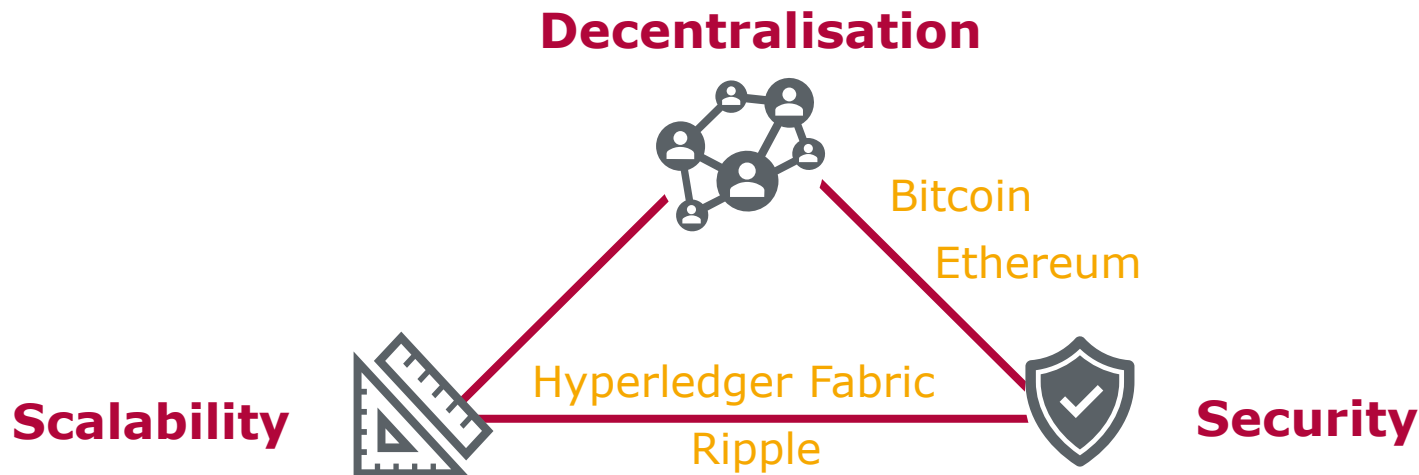
- In this context, we often speak about the so-called **trilemma**, we can **only have two** out of three aspects
- With **efficiency in our case**, we mean one of the most important properties of decentralized networks besides security, namely **scalability**
- It is **measured by** how the **performance varies** when the system is **resized** and whether the **system can grow without loss**



Scalability Trilemma

The term **scalability trilemma** introduced by Vitalik Buterin, co-founder of Ethereum, fits very well here

- It states that we can **only have two out** of either **decentralization**, **scalability** or **security**, so trade-offs are almost unavoidable
- All three are desired, but **only two can be ensured simultaneously**, the third aspect will see a dramatic decrease



Decentralization

The trilemma says that one possibility to increase scalability is to reduce decentralization

- That means the system can be more scalable if there are some users with more rights
 - As discussed in the previous video by example of Proof-of-Authority (PoA)
- In the blockchain scene, it is called the **degree of decentralization**
- Here we will **not** consider the **advantages** and **disadvantages** of decentralization since our **original goal** was a decentralized peer-to-peer network
- There are **enough alternative solutions** that play with the degree of decentralization in order to increase the scalability

In an attempt to make blockchain-based system “**more efficient,**” either the decentralization or the security of the system gets lost

■ **Security** in this context **can not be discarded**

- Scalability can be **traded for decentralization**
- Decentralization can be reduced for increase in scalability
 - “**degree of decentralization**”

