



openHPI Course: Blockchain – Revealing the Myth

Summary

Prof. Dr. Christoph Meinel
Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

Learning Objective of our Online Course

- **Congratulations**, you have reached the end of our online course
- We are pleased **that you have accompanied us**
- The **learning objective** of our online course was **far beyond** just explaining the technology behind the blockchain term
- We confronted the **hype problem** of the technology, which is surrounded by “myths”
- With that in mind, **we started the unveiling of the myth** of blockchain technology **at its cornerstone**, the **concept** of the **Bitcoin system**
- We have addressed the **underlying issues that led to the creation of the Bitcoin system** and each of its individual functionalities



Definition of Blockchain Technology Uninfluenced by its Alternatives

- This allowed us to work out a **definition of blockchain technology**, uninfluenced by its alternatives and adaptations
- From this, we have internalised the **following advantages that technology offers us**:
 - **Permissionless** and **secure peer-to-peer** network
 - **Without the need** for a **trusted third party** and
 - That does **not require trust between peers**

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

Ethereum was the Answer to the Needs of Post Bitcoin Projects

With the insight into **post Bitcoin projects**, we have gained the **impression of what** the users and developers of blockchain-based solutions **were missing in the technology** at the time

- **These needs** have been **successfully implemented** by the **Ethereum developers** in their system
 - Building a new **independent blockchain solution** on top of an existing blockchain
 - Using **flexible** and **complex scripts** and
 - Building a solution on top of an existing blockchain with **advanced features** that are not yet implemented within the existing blockchain



ethereum

What has changed?

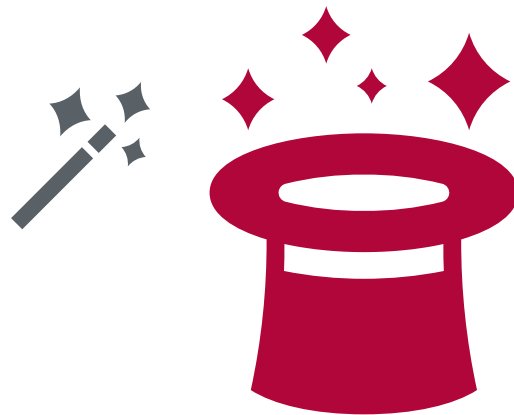
- After looking at the **Ethereum** solution **in direct comparison** to the **Bitcoin** solution, we found that the **scope of the technology** has changed
- It is **no longer limited to** the field of cryptocurrency or decentralized registry (**UTXO based**), but programmable, decentralized trust infrastructure (**account based**)
- But the **basis** and **idea**, as well as **advantages** that a blockchain-based system provides us with, have **remained unchanged**:
 - **Permissionless** and **secure peer-to-peer** network
 - **Without the need** for a **trusted third party** and
 - That does **not require trust between peers**



Real Challenge of Blockchain-Based Systems

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

- So, we have kept in mind the **real challenge of blockchain-based systems** and that is **scalability**
- So that was the **actual unveiling of the myth**
- Finally, we saw how we can **turn** the **theoretical understanding** we have gained **into concrete solutions**



Unanswered Questions

Perhaps **some questions remain unanswered** for some learners, e.g.,

- **Questions** that are **increasingly fuelled by hype**, such as
 - that **blockchain-based systems**, especially the best-known **Bitcoin**, are increasingly and largely **used for illegal transactions** and are **more suitable for criminals**, or
 - that the **Bitcoin** or **Ethereum price** and its **volatility**, is **determined by the underlying** blockchain **technology**
 - among the most widespread headlines is the **energy consumption of the Bitcoin system**



Blockchain-Based Systems are Illegal

To finally **separate the technology from the hype**, let's briefly address these common questions

■ **Blockchain-based systems are illegal:**

- The system itself and underlying technology **do not distinguish** whether it is used **for legal or illegal** purposes
- I.e., it has **no profit** from being used illegally
- Just like **gold** or various **fiat currencies**, such as the euro or the dollar
- **Censorship resistance** of blockchain-based systems may in fact **arouse the interest of criminals** to remain undetected



Bitcoin or Ethereum Price

Bitcoin or Ethereum price is determined by blockchain technology:

- We have learnt that **new Bitcoins** are **mined** and **distributed** to the miner **as a reward**
- I.e., if you are not a miner, you would probably **buy Bitcoins** on a **cryptocurrency platform** in exchange for your fiat currency (Euro)
- The **cryptocurrency platforms** have **nothing to do with** the Bitcoin system itself or its technology
- So, the **Bitcoin** or **Ethereum price** is determined by **supply** and **demand**
 - if the **demand** for Bitcoin **increases**, its **price rises**
 - if it **decreases**, the **price also decreases**



Energy consumption:

- **PoW**, as we already know, is **part of the security mechanism** of the Bitcoin system
- **Another part** of the mechanism is the **difficulty target for PoW**
- With the **increasing interest in bitcoin mining**, with the **aim of getting rewards** for it
- Then the **blocks are mined faster and faster**



Energy Consumption of the Bitcoin System (2/2)

- ...
- If the system's **limit of 10 minutes is passed**
- Then the **difficulty target** of the PoW **increases**
- Which automatically means the **hardware of miners** has to **search even longer** for the right solution or **upgrade the hardware**
- This leads to **increasing energy consumption**
- I.e., the **technology does not presuppose** immense energy consumption, **it is not specified** somewhere to consume so and so much
- **Miners alone** bear the **responsibility** for the decision to **keep upgrading**



Thank you for your interest!

**Feel free to share your experiences and
thoughts on this questions with other learners
in our forum**

