openHPI Course: Blockchain – Revealing the Myth

When to Use Blockchain Solutions

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

A Sober Fact Check

Now we have **not only** learned about the **technical aspects** of blockchain technology, but also about the **original problems** and **ideas** that **called for these technical measures**

- Following a step-by-step approach and exploring the **ideas** from the **Bitcoin concept**, we have **developed a definition** for a blockchain-based system
- We have also **reflected** on our **definition** after **exploring** the blockchain evolution to the **Ethereum** system
- We have **contrasted** what we have learned **with** the so-called **alternatives** of blockchain technology and the **challenges** that have led to these alternatives

A Sober Fact Check

Now we are ready to take a **sober look** at the
possible areas of application of blockchain technology

Which Application Needs which (Blockchain) Solution

Imagine an **arbitrary application** with **numerous users** and/or parties **that want to interact together** but **do not trust each other**

- Which of the **following solutions** would you prefer for **this application**?
  - a **robust** and **highly efficient** solution with **limited user permissions** (scalable and secure) or
  - a **robust** solution **without intermediaries and a central authority** (decentralized and secure)

Private Blockchain / Non-Blockchain-Based Distributed / Centralized Systems

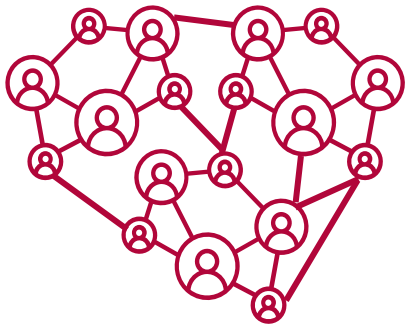
Following approaches would meet the requirements of the **first alternative** – scalable and secure

- A **private**, **permissioned blockchain**, e.g.,
  - proof-of-authority (a group of trustworthy validators secures the system)
- **Non-blockchain-based distributed** system, e.g.,
  - a distributed database system or
  - solution such as the Web of Trust
- A **centralized system**, when the central issue is the trust to be placed in a third party, e.g.,
  - public key infrastructure (PKI)

Public Permissionless Blockchain

Following approaches would meet the requirements of the **second alternative** – decentralized and secure

- A **public permissionless blockchain**
- Then one has to define **additional criteria**
  - **cost-benefit ratio** (size of the system, the existence of a separate IT team, etc.)
  - based on this, one need to decide whether an **existing solution** should be used, or an **own solution** should be developed
  - next question concerns the **actual objective of the application**



Public Permissionless Blockchain
Objective of the Application

What is the **objective of your application**?

- Is its focus that **a state** or more precisely the **possession of a value** must be securely **recorded** and **logged**?
  - Here, a simple **UTXO-based** blockchain is sufficient
- Is the application **more complex**? E.g.,
  - Are the states of a value or individual user accounts needed to **offer greater flexibility**? Or
  - Are the interactions of the users associated with **complex conditions** that are to be **automatically controlled** and **executed**?
  - Here, an **account-based blockchain 2.0** is the better choice

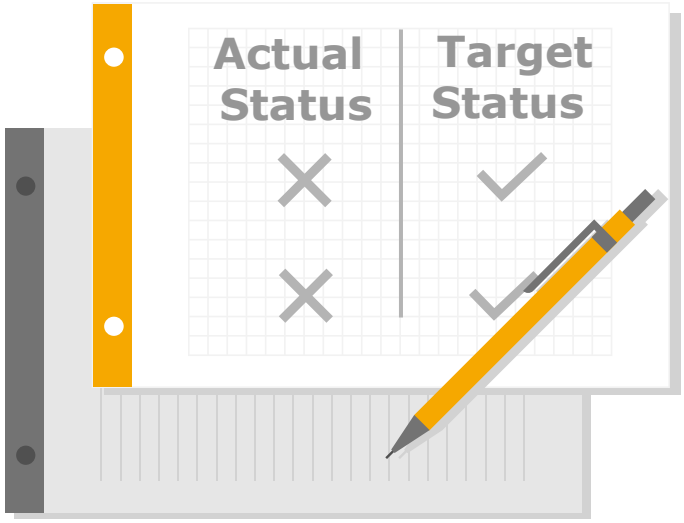
Account-Based Blockchain 2.0 …

… enable the system to act as a **large decentralized computer** with millions of **autonomous objects** (smart contracts)

- By means of these smart contracts, one can create **any complex application**
- Such so-called **decentralized applications**, or dApps for short, can be **controlled** and **used** in a **decentralized manner** without further intermediaries
- More complex smart contracts can represent so-called **decentralized autonomous organizations** (DAO) whose functions are executed automatically depending on predefined conditions

Summary (1/2)

- Whether you need a **highly scalable** or a **decentralised solution** **depends** on the **specific problem** to be solved
- It is necessary to **contrast** the **focus** of the **intended application** **with** the **possibilities** of the **respective technological solution**
- Only then is it decided whether it would be better to have a solution **with or without blockchain**



Summary (2/2)
Existing or Unique Solution

Choosing between an existing model or individualized solution

- Numerous **consortia** and **projects** have emerged that **support** other companies in **developing**, **testing**, and **providing** blockchain-based applications
- **Multiple application areas** have already been conquered by blockchain technology and more and more companies offer **ready-made solutions** that are **tailored to specific areas**
- As the **source code** of many blockchain-based systems **is public**, one can freely **use it** for your own blockchain applications and adapt it accordingly