openHPI Course: Blockchain – Revealing the Myth

Post-Bitcoin Projects and Evolution to Ethereum

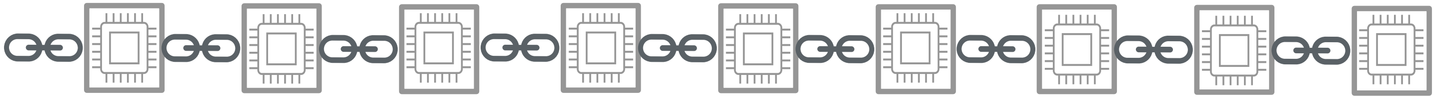
Prof. Dr. Christoph Meinel

Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

Post-Bitcoin Projects

- **Detailed description** of the Bitcoin concept and its **technical implementation** (Bitcoin protocol and software) are public
- Any developer around the world can **review the code** or make his own **modified version** of the Bitcoin software
- Thus, **two paths** have been established for the development of post-Bitcoin projects:
  - building an **independent blockchain** network and
  - building a solution **on top of Bitcoin**



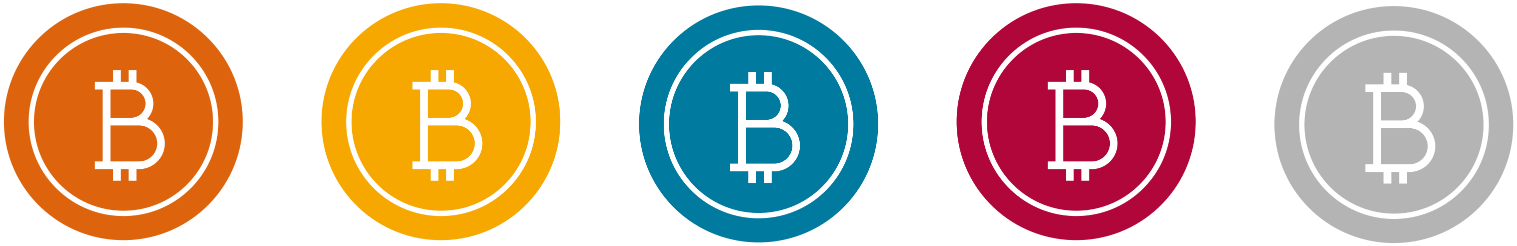
Post-Bitcoin Projects
Independent Blockchain Network

- Implementation of an independent blockchain-based system offers **greater flexibility** and **freedom in the composition** of the desired **functionalities** and **rules**
- However, at the **expense** of the **development time** and **security**, since changes to the existing solutions can lead to security gaps
- In addition, numerous applications that would make sense to implement, using blockchain technology, would be **too small to warrant their own blockchain**
- Independent blockchain solutions **lack interoperability**. For many decentralized applications, it would make sense if they could **interact with each other**

Post-Bitcoin Projects on Top of Bitcoin

To keep **development costs** low, many developers have decided to use the **existing Bitcoin system** to build their **solutions on top**

- Since the complexities of **mining** and **networking are already handled** by the Bitcoin protocol
- The most common mechanisms to realize this were **colored** and **meta coins**

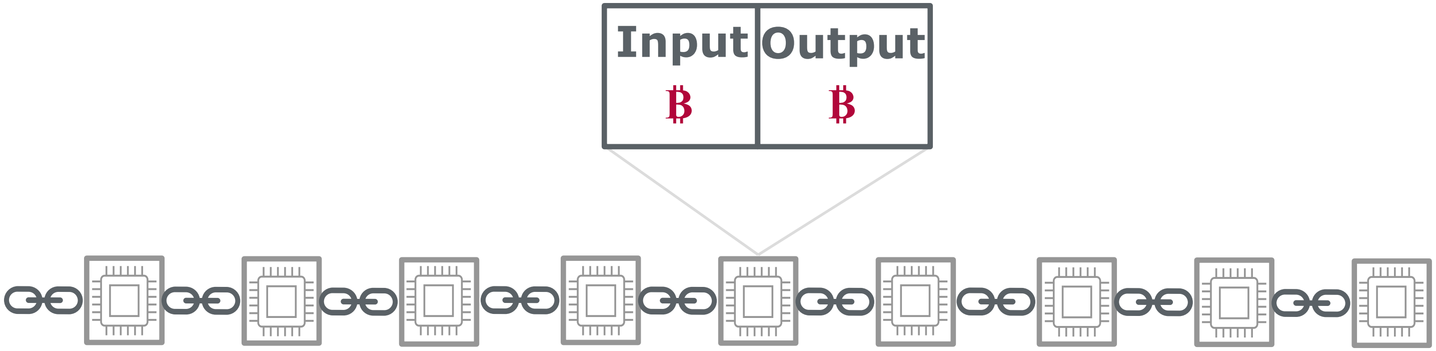


Post-Bitcoin Projects on Top of Bitcoin – Colored Coins (1/3)

- **Purpose of colored coins** is to allow people to create **their own digital currencies** or **digital tokens** that represent a **new value** such as a certificate, a share of a stock, a movie ticket, a rental apartment, or a digital key for a house or a car, on the Bitcoin blockchain
- The principle of colored coins involves **adding** to the already available bitcoins (i.e., to **UTXO**), additional information **(metadata)**

Post-Bitcoin Projects on Top of Bitcoin – Colored Coins (2/3)

- Becoming linked to this information, the **original Bitcoins become "colored"** and acquire a **different semantic**
- Mechanism **recursively distributes the color** of other UTXO
- Users who exchange colored coins (colored UTXO) use a **colored coins application** and know **what value** or **what property** the coins have
- They can send them around **like regular bitcoins**, **backtracking through the blockchain** to determine the color of any UTXO that they receive



Post-Bitcoin Projects on Top of Bitcoin – Colored Coins (3/3)

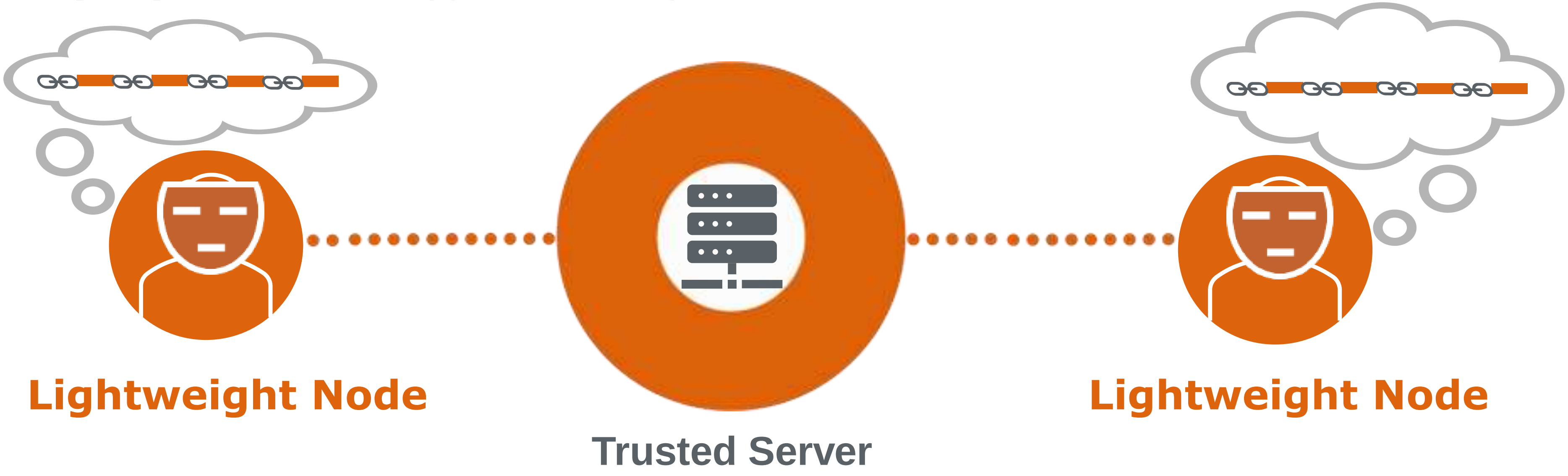
- However, the blockchain **miners cannot recognize the "color"** of the colored coins and see all incoming transactions as standard transactions
- For this reason, the added information (**metadata**) must be **verified** by those who use colored coins

Post-Bitcoin Projects on Top of Bitcoin – Meta Coins (1/2)

- **Meta coins** can provide, additionally to the **"new" value**, **advanced features** that cannot be implemented inside of Bitcoin itself
- The **idea behind** a meta coin is to have a solution that lives **on top of Bitcoin**, using Bitcoin transactions to **store meta coin transactions**
- For **Bitcoin miner** this transactions still looks like Bitcoin transactions
- So, the miners can't notice if the **meta coin transactions are not valid** under their own rules

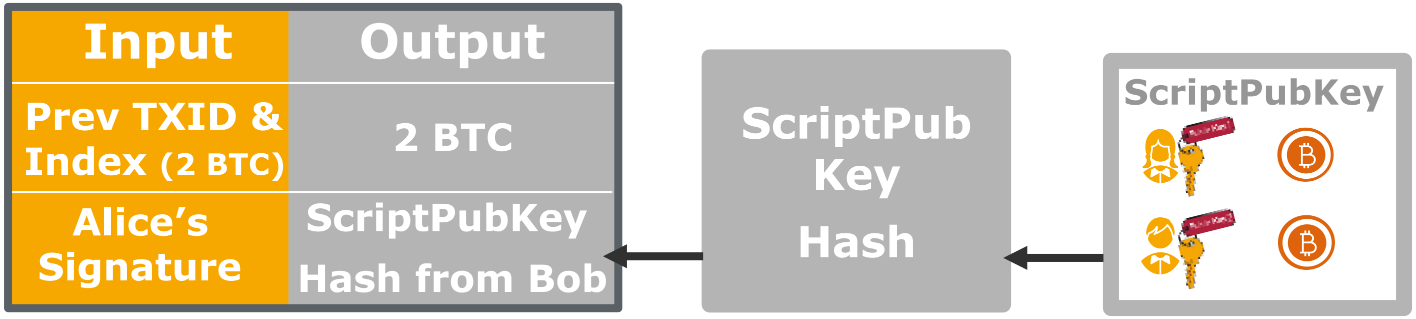
Post-Bitcoin Projects on Top of Bitcoin – Meta Coins (2/2)

- This makes the possibility of **simplified payment verification** difficult (store only the block headers as a light user)
- At the time of post-Bitcoin projects, all **"light" implementations** of Bitcoin-based meta-solutions rely on a **trusted server** that provides the data
- This is highly suboptimal, in particular, with regard to the **primary purposes** of a cryptocurrency to **eliminate the need for trust**



Post-Bitcoin Projects
Scripting on Top of Bitcoin

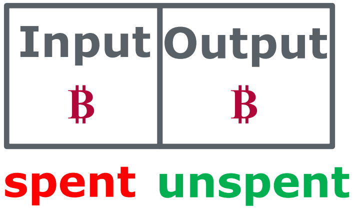
- You may remember the topic of **scripting**, which allows **greater flexibility** in the Bitcoin solution
- With the help of scripts, **UTXO** can be linked to **conditions**
- There are **different scripts** for various additional use cases
- However, the **scripting language** as implemented in Bitcoin has some **important limitations**
- This makes it **less flexible** for more complex solutions
- One of these important limitations is **lack of state**



Input	Output
Prev TXID & Index (2 BTC)	2 BTC
Alice's Signature	ScriptPubKey Hash from Bob

Post-Bitcoin Projects
Scripting on Top of Bitcoin – Lack of State

- Bitcoin system does **not provide account balances**
- It's more about **updating the state of the current ownership** of the coins
- More precisely, whether a bundle of coins is **spent or unspent**
- So, we only consider the **UTXO as valid coins**
- At the time of post-Bitcoin projects there is no opportunity for **multi-stage programs or scripts** which keep any other internal state beyond that
- It also means that **UTXO** can only be used to build **simple, one-off programs** and not more complex solutions



Input ₿ **Output** ₿

spent **unspent**

Intent of Ethereum

- **Ethereum** has gone a big step beyond the **usual approaches** tried so far
- **Ethereum founders** have not attempted to build a new UTXO blockchain or to build a solution on top of the existing Bitcoin system with limited capabilities, but to **merge these concepts**
- Ethereum system enables the **following approaches**:
  - □ 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

Summary

- Since the concept of the Bitcoin system as well as its technical implementation are public, **numerous new blockchain-based solutions have emerged** with modified Bitcoin software
- It was possible to develop **either an independent new blockchain-based** system **or one on top of Bitcoin**
- Ethereum system enables 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**