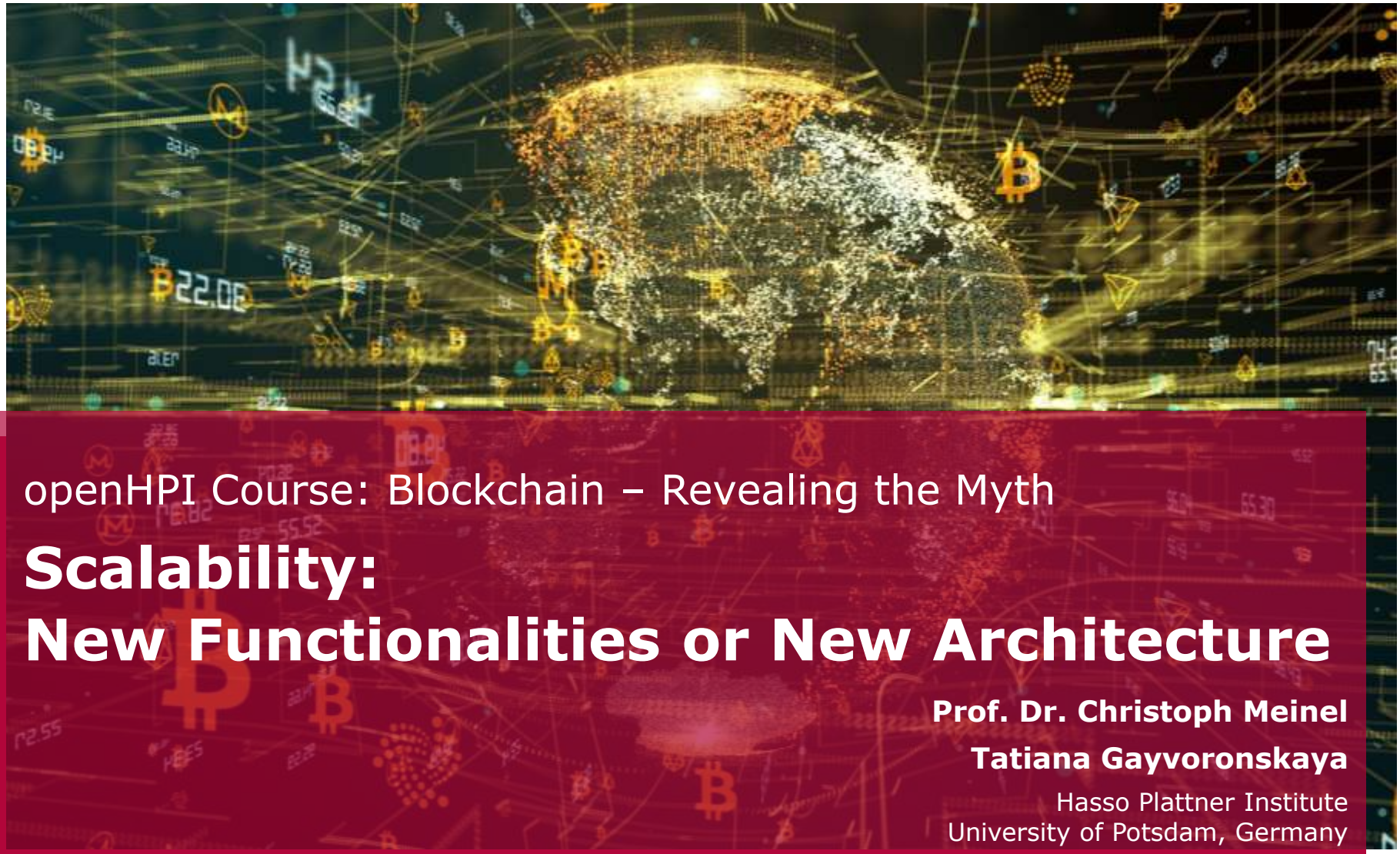


openHPI Course: Blockchain – Revealing the Myth

Scalability: New Functionalities or New Architecture

Prof. Dr. Christoph Meinel

Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

New Functionality for Better Scalability of the Bitcoin System

In the last clip we mentioned that **fundamental changes in the blockchain protocol** like modification of block size or block time would …

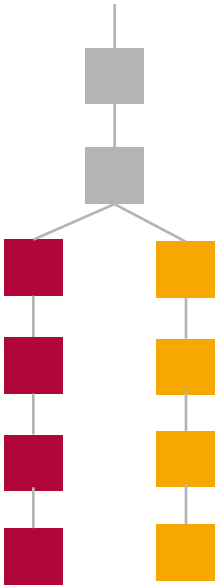
- require the **acceptance by all miners** and **all users**
- and those **who don't accept** the changes are **"split off"** from the **system**

Indeed, a new cryptocurrency called **Bitcoin Cash (BCH)** was created **through such a split** on August 1, 2017

- It introduced **8 MB blocks** instead of the existing **1 MB**

Another group in the **Bitcoin community** chose to take a **different path** in solving the block size problem

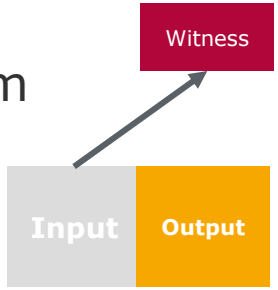
- Instead of changing the protocol, they introduced a **new functionality** called "**Segregated Witness**" or shortly **SegWit**



New Functionality for the Bitcoin System Segregated Witness

The **advantage** here is that **users can be updated at any time**, after the **miners** have **accepted** the changes

- Miners and users, **who have not yet updated** the new functionalities, **continue to belong to the same** system as the updated users
  - they only see an **"extra text"** that they **do not understand**
- However, this does not pose a problem as **it does not mean any changes** to the fundamental rules
- The **focus** of the new functionality is a **new data structure called Witness**
- A part of the transaction is "**moved**" **therein**, namely the **signature**, which otherwise makes up to **70 percent** of a transaction



New Functionality for the Bitcoin System Witness

"**Witness**" still remains **part of the transaction**, but is **not hashed** in the **transaction ID**

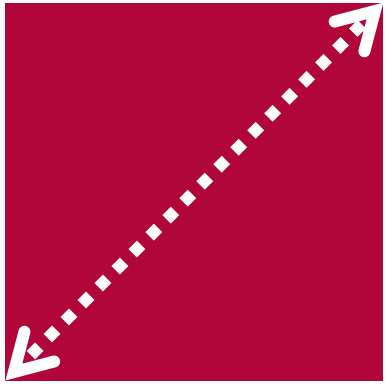
- **Users** who have **not yet implemented SegWit** think that SegWit transactions **do not have a signature** (in the ScriptSig) and **do not require one** (in the ScriptPubKey)
- **Updated users understand the instructions** in the ScriptPubKey and **know** that the **necessary signature** is in the "**Witness area**"

Not updated user **Updated user**

New Functionality for the Bitcoin System Increasing Block Size

But how the **size of the transaction** is **decreased** if **Witness** still **remains part of the transaction**?

- **Block size limit** in the Bitcoin system **remains unchanged** at 1 MB after the SegWit update
- **Block size** is replaced by "**block weight**," and the block can have a "weight" of between 2 and 4 MB



Limits to What the Bitcoin System Can Currently Handle

This means, the current full nodes **need more time than before to verify a block**

- This correspondingly **increases** the **block's spread time** in the system
- SegWit supporters consider, that the **additional verification time** and the **associated longer propagation time** for a block **lie within the limits of what the network can currently handle**

Ethereum Has Also to Struggle With a Larger Amount of Data

What about the Ethereum system, which has to struggle with a **larger amount of data** than the Bitcoin system?

- In this sense, the **account-based** Ethereum system has a considerable **advantage over** the **UTXO-based** Bitcoin system
- When **verifying a transaction**, the **entire blockchain** is **no longer searched** for an output, which is referenced in the current input
- Instead, the **current state** of the **respective account** (account state) is checked as to whether it has a sufficient balance

Ethereum System
Long-Term Scalability Improvement

For a **long-term improvement** in **scalability** of the Ethereum system developers plan to create and introduce an **Ethereum 2.0** within the next years

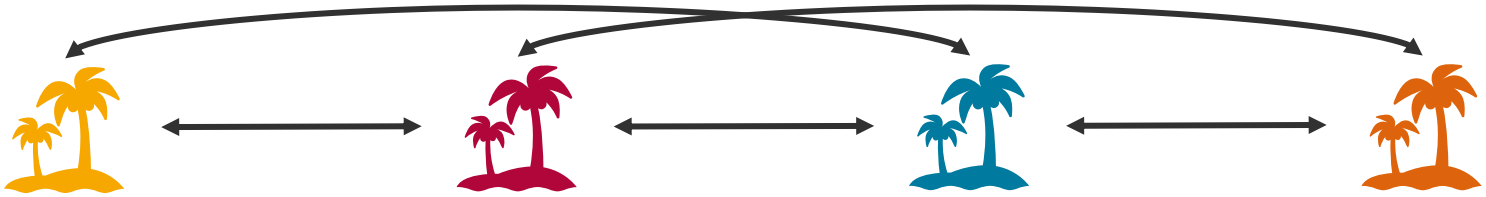
- Focus is on
  - **splitting** the entire system **into numerous groups** and thus
  - **dividing** the **transaction load** and
  - allowing **parallel calculations**
- **Entire architecture** of the Ethereum system is thereby "**rebuilt**" and can be displayed in **several layers**

Ethereum 2.0 Architecture
Sharding

Let us take an **example** from Vitalik Buterin on this topic and imagine that the **Ethereum system** is **divided into thousands of islands**

- **Each island** has its **own functionalities** and **inhabitants** (user and smart contract accounts)
- **Inhabitants** of an island **communicate** with each other, **organize** themselves and have their **own transaction history**
- **Islands** can **interact** with each other

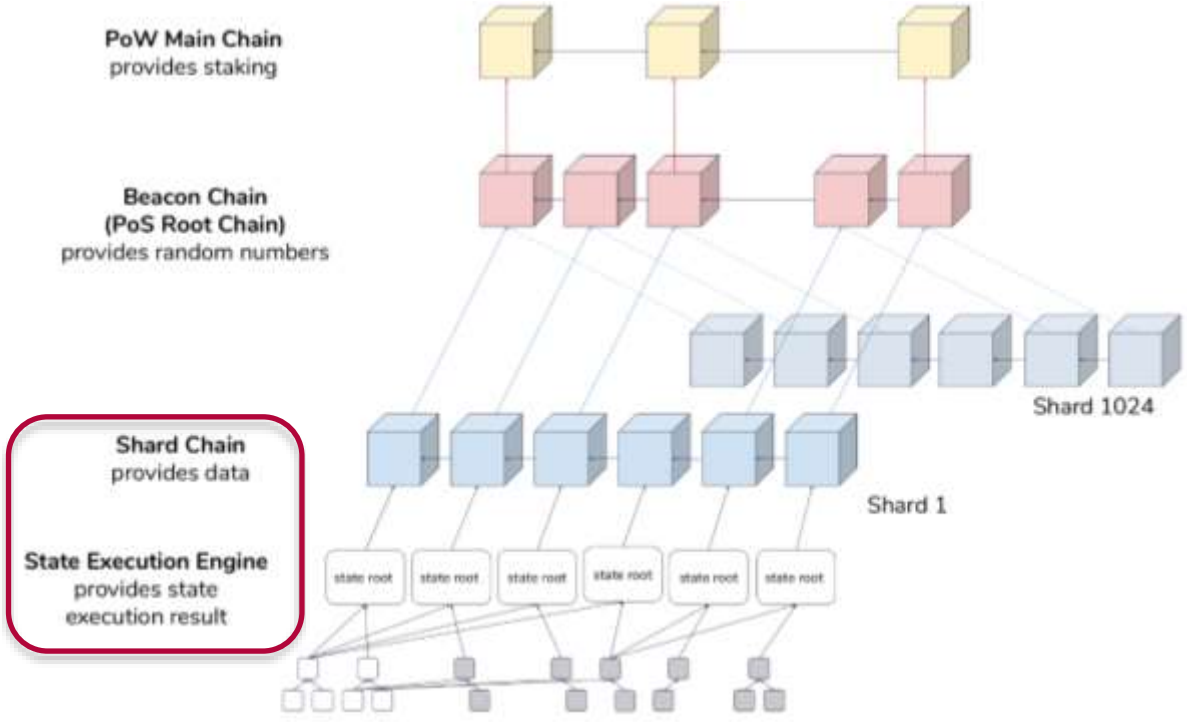
This procedure is called **sharding** and the "islands" are correspondingly called "**shards**"



Ethereum 2.0 Architecture
Data and Execution Layers

Shards represent **the two lowest layers** of this new architecture: the **data** and **execution layers**

- The **transactions** and **smart contracts** are executed and saved **for each shard**

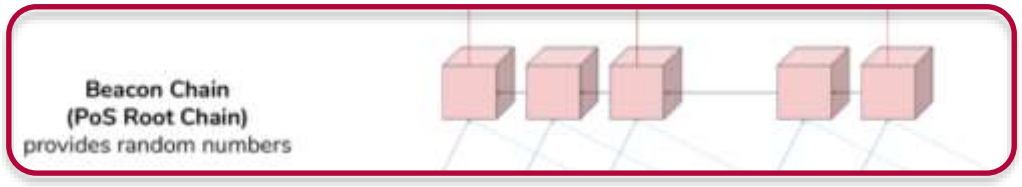


Source: Hsiao-Wei Wang – Presentation "Ethereum, Serenity"

Ethereum 2.0 Architecture
Coordination and Validation Layer

Next layer is used to **coordinate** and **validate** the **data produced in the shards**

- It consists of a **new blockchain** – a so-called **beacon chain**, which uses a **PoS algorithm**
- Miners are replaced by validators, which have the **possibility to create a block in a shard** that has been randomly assigned to them
- For each shard, a **group** made up of **100** randomly selected **validators**, authenticate the new block by signing
- **Block header** is included in the **beacon chain block** with at least 67 signatures as **references to the shard block**

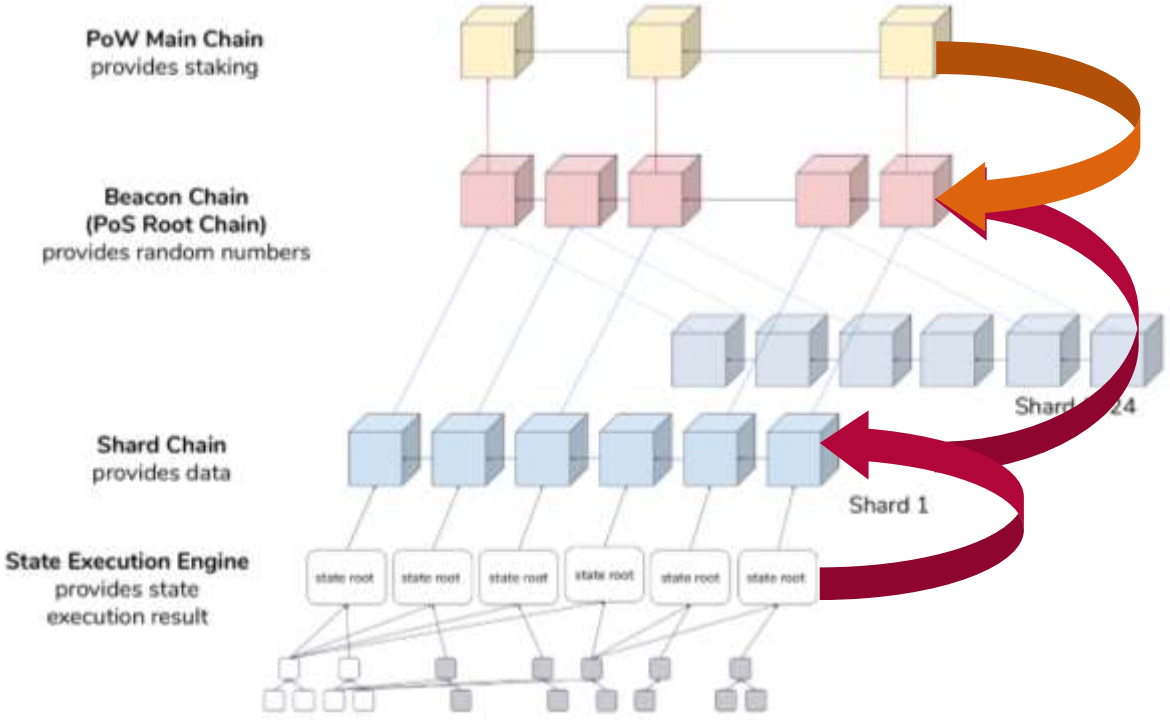


Source: Hsiao-Wei Wang

Ethereum 2.0 Architecture
Top Layer

The **current Ethereum blockchain** remains available, uses **PoW** and represents a **top layer**

- **Any Ethereum user** who stores 32 Ether in form of a smart contract in the Ethereum top layer **can be a validator**



Source: Hsiao-Wei Wang – Presentation "Ethereum, Serenity"

Summary

We have considered **various ways** to make a **blockchain-based system a bit more "efficient"**

- **Adjusting parameters** such as block time and block size
- **Introducing additional functionalities** that avoid changing the set parameters or
- **Completely new architecture** that still has a PoW blockchain as its basis

In the next clip we look at a **last scaling option**, that intends to relieve the system, so-called **off-chain approach**