openHPI Course: Blockchain – Revealing the Myth

Bitcoin: Recap

Prof. Dr. Christoph Meinel

Tatiana Gayvoronskaya

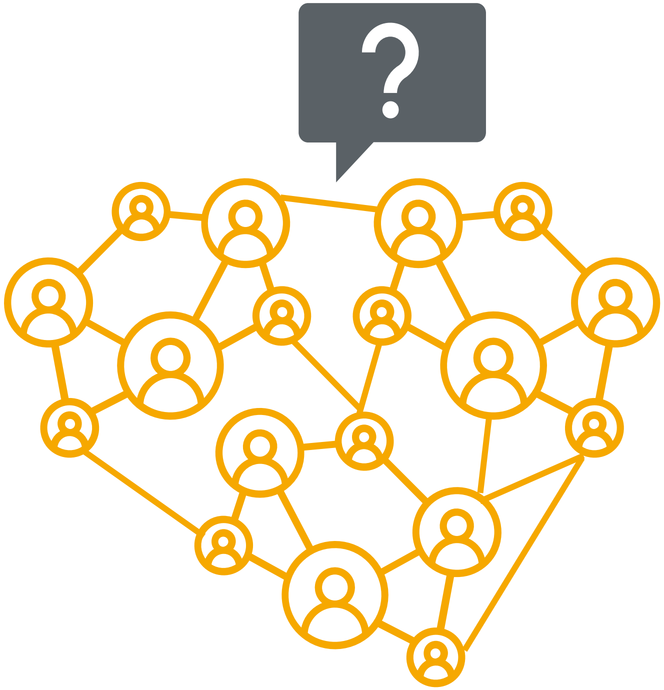
Hasso Plattner Institute
University of Potsdam, Germany

Bitcoin Solution

- In compact **7 steps** we have covered the complete **complex Bitcoin solution**
- We started with the **origin problem**: *"How can we take advantage of paying by physical currency on the Internet without a trusted third party?"*
- And continued with **concrete individual solutions**:
  - □ **Framework of coins** made from digital signatures
  - □ A system for participants to agree on a **single chronological order** in which transactions were received
  - □ Solving the **double-spending** problem by a peer-to-peer distributed timestamping
  - □ **Incentivizing** users to comply with the rules and to provide a proof-of-work
  - □ Making the Bitcoin system **more flexible**

User’s and System’s Perspective on the Advantages of the Bitcoin System

To better understand **what advantages** the system offers compared to other solutions, let's have a look at this system from the **user's perspective** and from the **system's perspective**



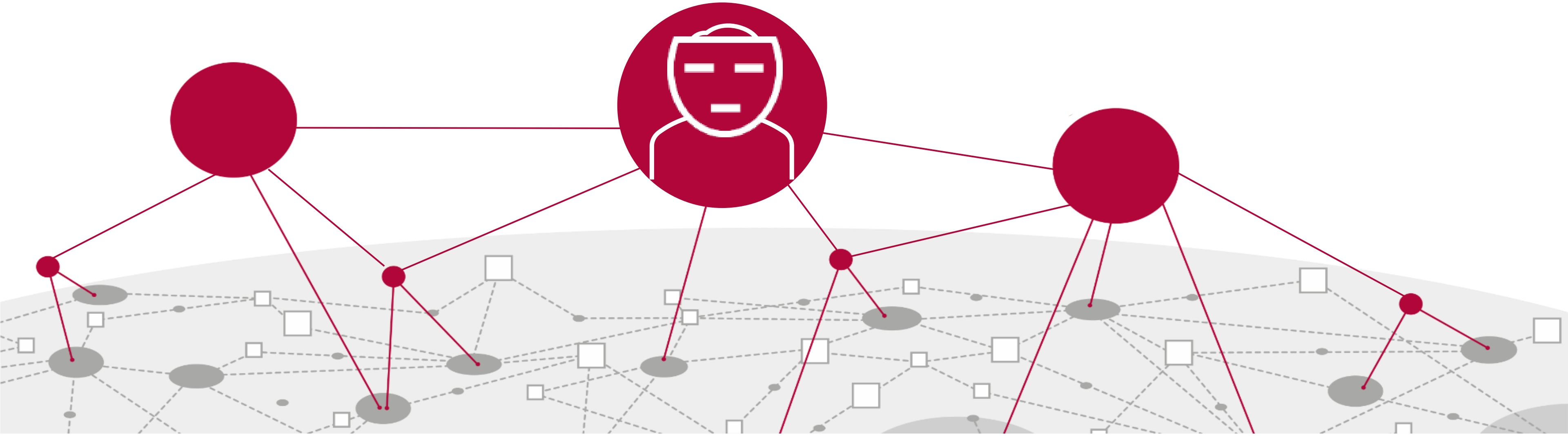
Advantages of the Bitcoin System
User Perspective (1/2)

An electronic payment system, allowing any two willing parties to transact directly with each other without the need for a trusted third party

- Users do not have to meet any conditions joining the system
- To use the system, user only need to use the corresponding app (for full or lightweight user)
- Besides containing all rules and functions the app also has a database with a copy of all resources (all blocks with transactions or only block headers with respective transactions)
- When users join or rejoin the system (when starting the app), the database is updated by loading the missing information
- In this way, the app communicates with all the other users' apps. All data are exchanged (transactions, blocks), the data are checked and saved (only full users)

Advantages of the Bitcoin System User Perspective (2/2)

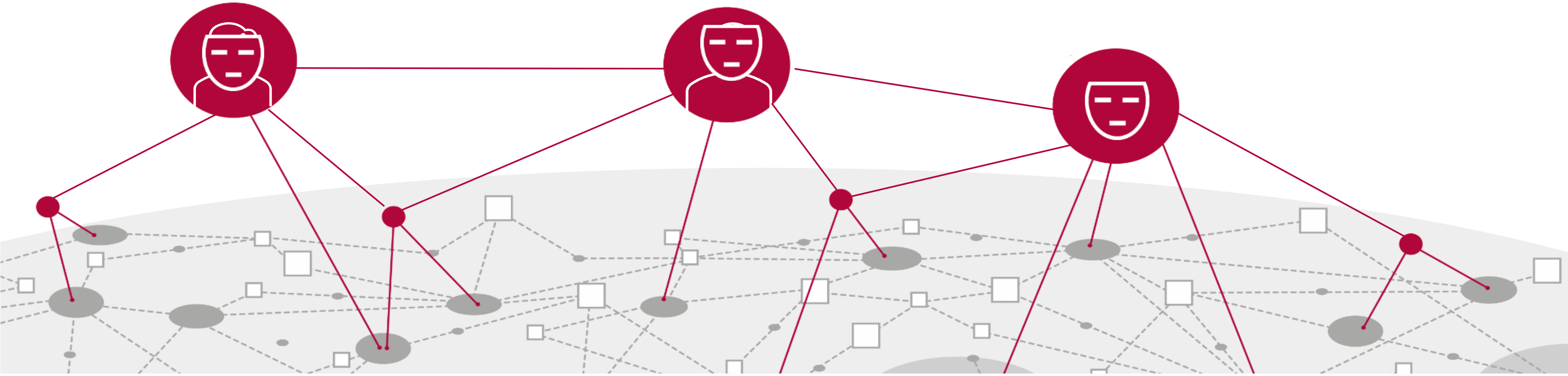
- Users are flexible in the choice under which conditions bitcoins may be spent
- Users can earn money by supporting the system and spending CPU time for work-of-proof to create new blocks
- Users can be sure that as long as most of the CPU power is in the hands of honest users, the system will remain free from fraud, independent of third parties and thus resistant to censorship



Advantages of the Bitcoin System
System Perspective: Network

A system for electronic transactions without relying on trust

- The network is robust in its unstructured simplicity
- Users work all at once with little coordination
- They do not need to be identified, since messages are not routed to any particular place
- Users can leave and rejoin the network at will, accepting the current state of the system (longest chain) as proof of what happened while they were gone

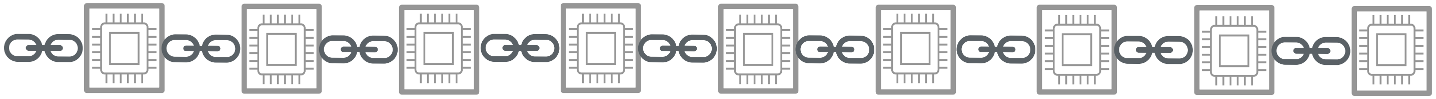


Advantages of the Bitcoin System
System Perspective: System – Order

- To avoid missing transactions, all transactions are publicly announced (in trust-based systems, this is regulated by a central authority)
- Cryptographic linking of contents determines the single chronological order in which contents (transactions, blocks) were received

Advantages of the Bitcoin System
System Perspective: System – Security

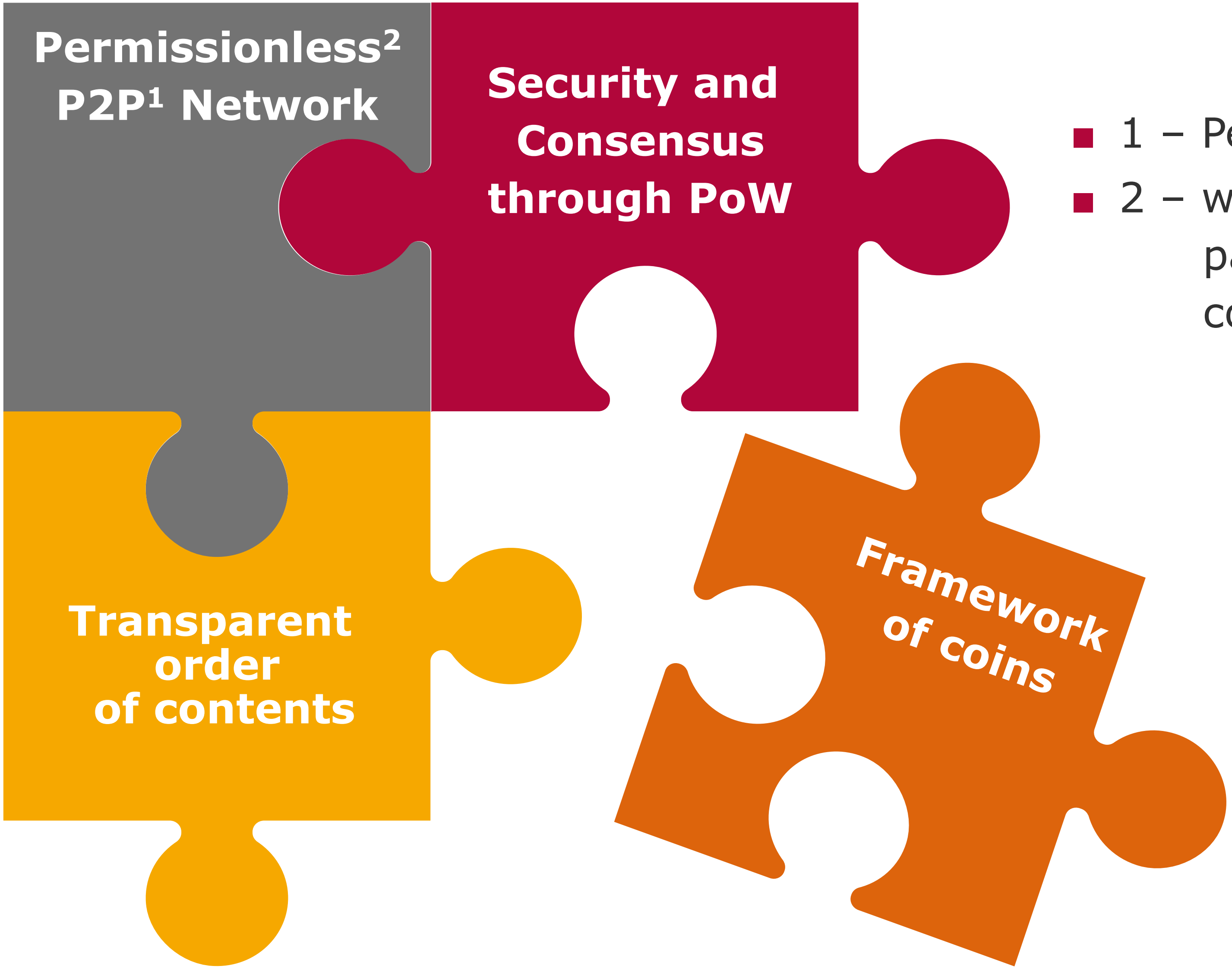
- For this single chronological order, users vote with their CPU power. The correct order will then be the one with the most votes (this has the greatest proof-of-work effort invested in it)
- This work deters the attackers as they have to redo the same work. They ought to find it more profitable to play by the rules
- The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes



Advantages of the Bitcoin System
System Perspective: Framework of Coins

- Framework of coins made from digital signatures, which provides strong control of ownership
- Coins in the system have the property of being spent or unspent (active coins represented by UTXO’s)
- Coins are mined decentraly

Advantages of the Bitcoin System
Separation into Individual Segments


Permissionless[2] P2P[1] Network

Security and Consensus through PoW

Transparent order of contents

Framework of coins

- 1 – Peer-to-Peer
- 2 – without participation conditions

Definition of Blockchain

Now let's try to define the underlying technology of the Bitcoin system, moving away from the field of cybercurrencies

- Feel free to share your ideas on a definition in the forum!

Blockchain technology provides a permission less peer-to-peer network using proof-of-work to record a public history of contents that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. This is done without any trusted third party and does not require trust between peers.

See also:
Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008

Summary

- Congratulation if **you have made it this far**
- After grasping the Bitcoin system now we **move** to other **application areas** to see how they can be disrupted by the **blockchain technology**
- In the next video we will explore the **evolution of blockchain technology** into a decentralized world computer