TECHNISCHE UNIVERSITÄT DARMSTADT

Seminar

Blockchain Technology

Dr. Rachid El Bansarkhani

Email: elbansarkhani@cdc.informatik.tu-darmstadt.de

Organisation

TECHNISCHE UNIVERSITÄT DARMSTADT

- Anmeldung über TUCAN

- Voraussetzung
  - Einführung in die Kryptografie
  - (ggfs: Trusted Systems, IT-Sicherheit, P2P,…..)

- Blockveranstaltung
  - In der zweiten Hälfte des Semesters
    (wird noch bekannt gegeben)

Organisation

TECHNISCHE UNIVERSITÄT DARMSTADT

- Themenauswahl
  - 5 Themenkomplexe
  - Jeder Student/Gruppe: 3 Vorschläge mit Prioritäten
  - Bis zum 21.04.2017 per Email an elbansarkhani@cdc.informatik.tu-darmstadt.de
  - Pro Thema gibt es 1-2 Treffen

Organisation

TECHNISCHE UNIVERSITÄT DARMSTADT

- Benotung
  - Präsentation (ca. 45min, 40%)
    [Abgabe ca. 1 Woche vor der Präsentation]
  - Ausarbeitung (ca. 10-15 Seiten/Person, 40%)
    [Abgabe ca. 2 Wochen nach der Präsentation]
  - Beteiligung (20%)
- Vorauss. Planung:
  - Thesis
  - Praktikum
  - Projekte

Ziel des Seminars

TECHNISCHE UNIVERSITÄT DARMSTADT

- Umfassender Einblick in die Thematik
- Frühe Auseinandersetzung
- Praxisnähe
- Vorbereitung auf zukünftige Herausforderungen und später im Beruf

TECHNISCHE UNIVERSITÄT DARMSTADT

2008 veröffentlicht unter dem Pseudonym

Satoshi Nakamoto

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 benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

TECHNISCHE UNIVERSITÄT DARMSTADT

Ziel/Herausforderung

Dezentraler Konsens mittels Kryptografie

Wie?

1. *Public Ledger: Öffentliches Nachweisbuch*
2. *P2P Netzwerk mit leistungsfähigen Knoten*

Funktionsweise

TECHNISCHE UNIVERSITÄT DARMSTADT

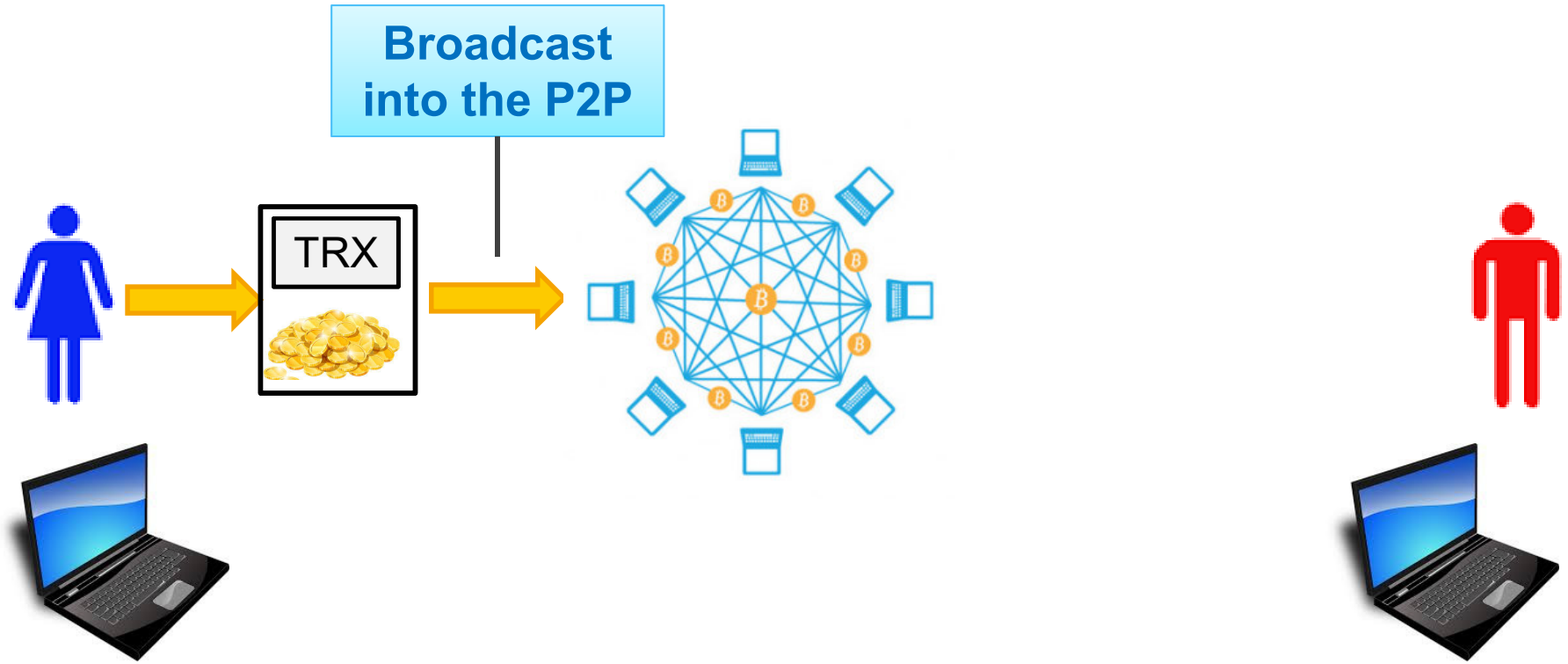
- *Keine zentrale Instanz* mehr notwendig
- *Kein Vertrauen* mehr notwendig, solange die Mehrheit der Miner ehrlich ist
- Basiert auf einem *P2P*-Netzwerk
- Zahlreiche Anwendungsgebiete in allen Branchen
- Erstes Blockchain Protokoll: **BitCoin**

BitCoin: Abstrakt

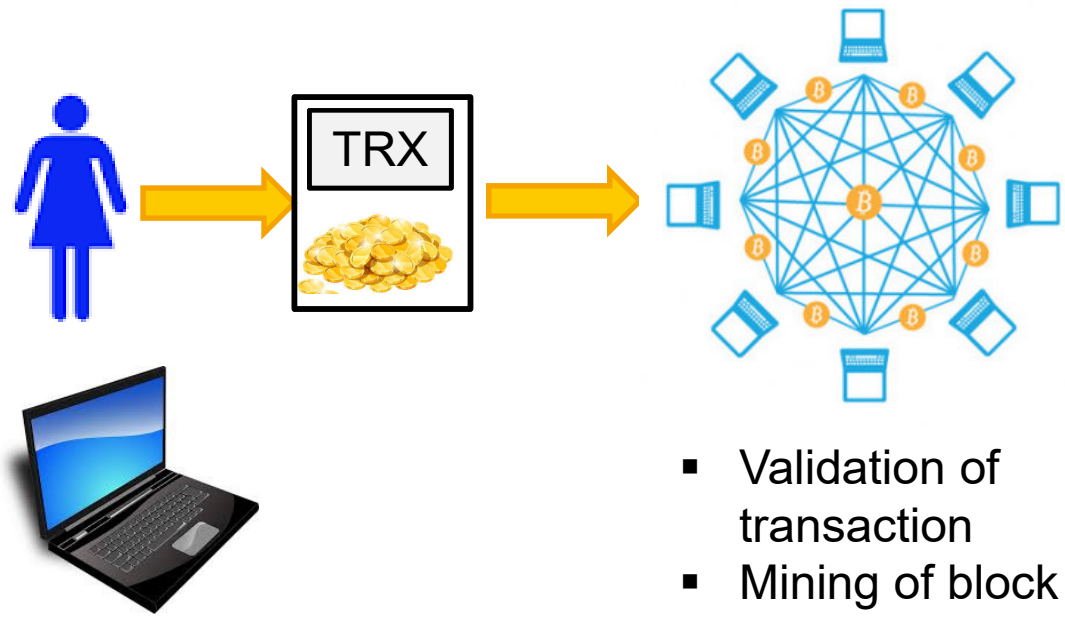
TECHNISCHE UNIVERSITÄT DARMSTADT

BitCoin: Abstrakt

BitCoin: Abstrakt

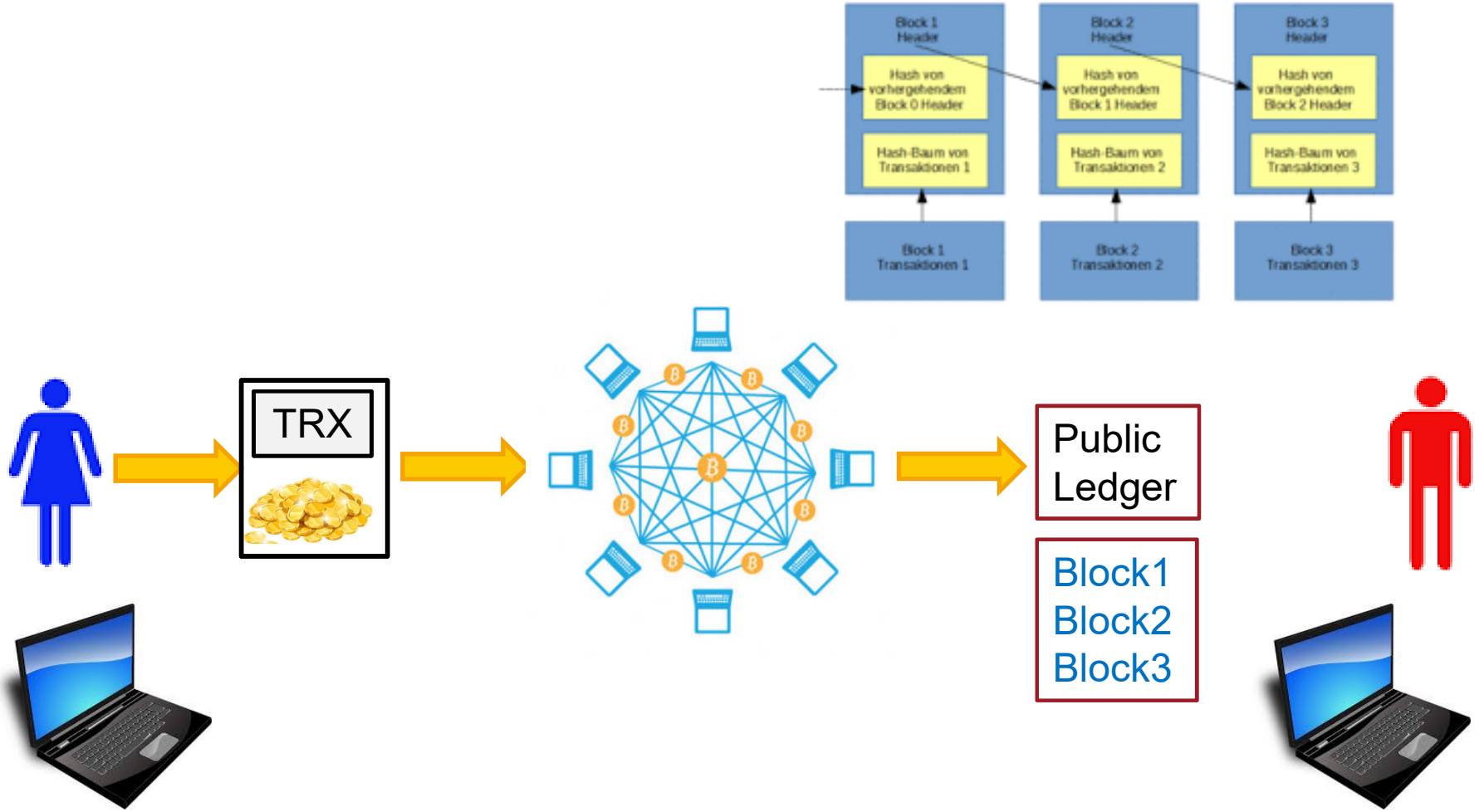


BitCoin: Abstrakt

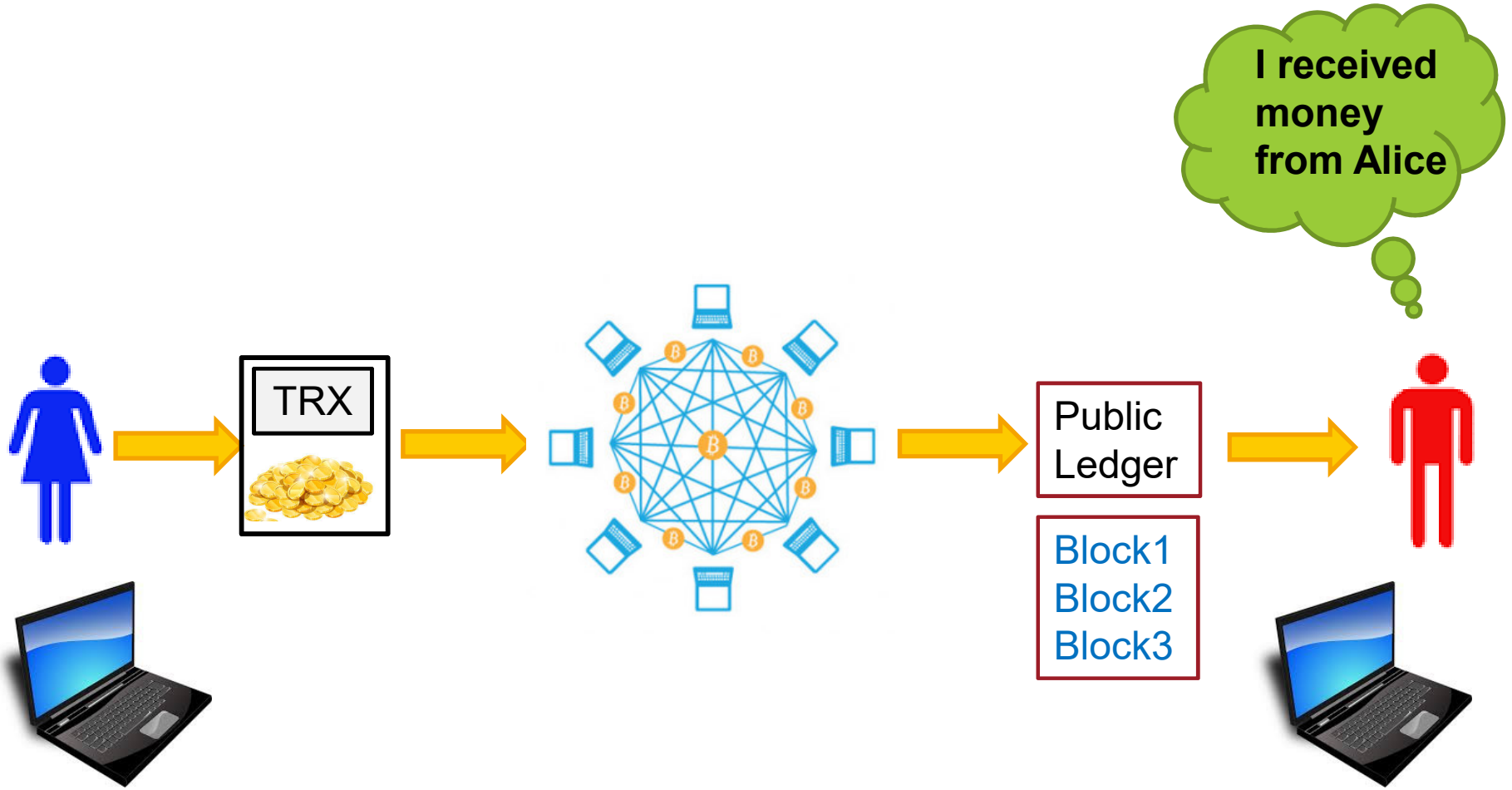


- Validation of transaction
- Mining of block 3

BitCoin: Abstrakt



BitCoin: Abstrakt



Themenkomplexe

TECHNISCHE UNIVERSITÄT DARMSTADT

- Funktionsweise
- Anwendung von Blockchain Technologien
- Protokolle und Sicherheitsmodelle
- Implementierung
- Attacken und Sicherheit

Funktionsweise

TECHNISCHE UNIVERSITÄT DARMSTADT

Wie funktioniert Blockchain?

- Ausführliche Beschreibung
- Welche Probleme werden gelöst und welche entstehen? Vorteile, Nachteile?
- Methoden zur Realisierung
  - Proof of Work, Proof of Stake, Proof of Elapsed time, Proof of Luck, Proof of Activity, Proof of Space, …
  - P2P

Anwendungen

TECHNISCHE UNIVERSITÄT DARMSTADT

Wie und wo kann man Blockchain Technologien einsetzen ?

- Überblick über verschiedene Anwendungsgebiete
  - Smart Contracts, Smart Properties
  - IoT, Pharma, Supply Chain Management, NameCoin, Finanzen, Notariat, …….
  - Viele Whitepapers im Internet
- Ausführliche Beschreibung von 2 -3 Anwendungen
  - z.B. im Bereich Supply Chain Management, Pharma, IoT

Protokolle und Sicherheit

TECHNISCHE UNIVERSITÄT DARMSTADT

- Wie ist die Sicherheit zu bewerten?
- Gibt es Sicherheitsmodelle?
- Aufbau und Annahmen?

Bsp:

1. Snow White: Provably Secure Proofs of Stake

2. Analysis of the Blockchain Protocol in Asynchronous Networks

Implementierungen

TECHNISCHE UNIVERSITÄT DARMSTADT

- Wie werden solche Protokolle auf Implementierungsebene realisiert?
- Wie kann man Smart Contracts/Properties realisieren, wie z.B. bei Ethereum?
- Wie kann man die Protokolle nutzen/adaptieren?
- Protokolle: Ethereum, SIA Blockchain, BitCoin NG, PeerCoin, Storj.io

Attacken und Sicherheit

TECHNISCHE UNIVERSITÄT DARMSTADT

- Welche Attacken gibt es auf Blockchainprotokolle?
- Gibt es Lösungen dazu?
- Bsp:

1. Tampering with the Delivery of Blocks and Transactions in Bitcoin

2. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin

3. On the Security and Performance of Proof of Work Blockchains

TECHNISCHE UNIVERSITÄT DARMSTADT

Thank you for your attention.

Questions?