Analysis of Use Cases of Blockchain Technology in Legal Transactions

Ulrich Gallersdörfer, 09.01.2017, Munich

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de
Outline

1. Motivation
2. Research Approach
3. A deep dive into BlockChain Technology
4. Research Questions and Contributions
5. Thesis Timeline
“Every informed person needs to know about Bitcoin because it might be one of the world’s most important developments.”
Leon Louw
Motivation

**Exchange Rate Bitcoin**

[Image: blockchain.info/de/charts/market-price]

**Google Trends “BlockChain”**

[Image: https://www.google.com/trends/explore?q=Blockchain]

**Twitter Post:**

@paultoo

Bitcoin may be the TCP/IP of money.

[Image: https://twitter.com/paultoo/status/328969714283995136]

**News Article:**

B3i: Allianz und andere Versicherungsriesen gründen Blockchain-Initiative

[Image: https://heise.de/-3355409]

Die Blockchain wird zum goldenen Kalb der Finanzwelt: Nach den Großbanken gründen nun auch die Versicherer eine eigene Initiative zur Erprobung der Blockchain-Technik.
Motivation

„Blockchains are overhyped.“
Gideon Greenspan, Founder / CEO of Coin Sciences Ltd.

We want:
⇒ Down-to-earth view on BlockChain technology
⇒ Deep understanding of underlying technology
⇒ Assessment of risks and chances of this technology

Setup of this Master Thesis

• **Title:** Analysis of Use Cases of Blockchain Technology in Legal Transactions

• **Author:** Ulrich Gallersdörfer ([ulrich.gallersdoerfer@tum.de](mailto:ulrich.gallersdoerfer@tum.de))

• **Advisor:** Bernhard Waltl ([b.waltl@tum.de](mailto:b.waltl@tum.de))

• **Start:** 15. November 2016

• **End:** 15. May 2017
# Outline

1. Motivation
2. Research Approach
3. A deep dive into BlockChain Technology
4. Research Questions and Contributions
5. Thesis Timeline
Research Approach

1. Research
   • Literature Research

2. Conceptual BlockChain Architecture
   • What is the blockchain and how can it be parameterized?
   • Which value do blockchains add to a enterprise architecture?

3. Guided interview
   • Understand enterprises' needs
   • Gather and structure usecases

4. Implementation
   • Implement a prototypical usecase

5. Evaluation
   • Evaluate use case and different scenarios
Outline

1. Motivation
2. Research Approach
3. A deep dive into BlockChain Technology
4. Research Questions and Contributions
5. Thesis Timeline
A blockchain […] is a **distributed database** that maintains a continuously-growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. **By design** blockchains are **inherently resistant to modification** of the data: once recorded, the data in a block cannot be altered retroactively.”

A deep dive into BlockChain Technology

BlockChain Overview

See further explanations on the whiteboard.
Picture of the Whiteboard

Diagram showing a flowchart with labeled nodes and a formula:

```
Header: TS + h(Data) + h(prev. B) + nonce
```

Additionally, there are symbols and numbers indicating data flow and connections:

- A → B → C
- 3
- 10 - 20
- 10 min
Outline

1. Motivation
2. Research Approach
3. A deep dive into BlockChain Technology
4. Research Questions and Contributions
5. Thesis Timeline
Research Questions

1. What are parameters of the blockchain technology?

2. What are usecases based on blockchain technology and which requirements emerge from them?

3. How can blockchain technology be integrated in enterprise architectures?

4. What are the risks of applying blockchain technology and how can they be minimized?
Preliminary Result: Blockchain Architecture

- Hardly any literature about a high-level overview on blockchain architecture
- Knowledge base to reflect in expert interviews
Preliminary Result: Blockchain Architecture

- **Business**
  - Provenance Tracking
  - Record Keeping
  - Multiparty aggregation

- **Business Service**
  - Service Providers

- **Application**
  - Persistent Data Storage
  - Integrity Assurance
  - Private/Public/Shared Ledger
  - Crypto Currencies
  - Bank Transfer
  - Asset Transfer
  - Copyright Protection
  - Proof of Publication
  - DRM
  - Smart Contracts
  - Computable Contracts
  - Electronic Insurance
  - Executable contracts
  - Trading algorithms (high volume, high speed)

- **Infrastructure Service**
  - Block Header
  - Transaction Trees
  - Puzzle/Mining Agreement
  - Transaction Input/Script(s)/Output/Script(s)

- **Infrastructure**
  - Distributed Network (e.g., P2P)
  - Public, Private, Shared
  - Hardware Devices/Mining Devices/IoT
  - Used Algorithms
  - Hashes
  - Digital Signatures
  - Strategies
  - Strategy fitted to client
Outline

1. Motivation
2. Research Approach
3. A deep dive into BlockChain Technology
4. Research Questions and Contributions
5. Thesis Timeline
Timeline of Master Thesis

Approach
- Literature Research
- Concept Development
- Interviews
- Concept & Implementation

Writing MA
- Writing
- Review

Research Questions

A ✓ B

November | December | January | February | March | April | May
---|---|---|---|---|---|---

Day 1

Concept

Day 2

Implementation

Day 3

Writing

Day 4

Review

Day 5

Literature Review
Backup

Ulrich Gallersdörfer, 09.01.2017, Munich

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de
Sources


Credit to icons:
Designed by Freepik and distributed by Flaticon
Blockchain Architecture

Focus

Layers

TI
Technical Interaction
Creation of transactions
Creation of scripts

AI
Abstract Interaction
Consensus
Storage of Transactions

DI
Domain Interaction
Propagation
Validation of Transactions
Block Building
Mining

DS
Domain Service
Storage, Integrity
(Keeping List of unspent transactions)

DD
Domain Data
Blocks & Blockchain
Concatenation

AD
Abstract Data
Transaction-Trees
Transactions
Scripts

TD
Technical Data
Data
Signatures
Hashes
Blockchain Architecture

Data Structure (BlockChain)
- Block
  - BlockHeader
    - Hashes
- Transaction
  - Scripting Language
  - DSA
- Genesis Block
  - Links to n-1
- Tree of Transactions
  - Are transferred
  - Defines

Methods
- Hash Algorithm
- Scripting Language
- DSA

Network
- Centralized
- P2P
- Paxos
- Consensus

Variables
- Blocksize
- Propagation Speed / Difficulty
- Wallet/Transaction based

Privacy Aspects
- Anonym
- Pseudonym

Stakeholder
- Investors
- Payment services
- Core Developers
- Creditor
- Debitor
- Miners

Mining
- Proof of Work
- Proof of Useful Work
- Proof of Stake

170109 Gallersdörfer Kick-Off Master Thesis