Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

**BACHELORARBEIT**

# Blockchain-Technologie im Online Advertising

vorgelegt von

Daniel Braun


| | |
|---|---|
| Fakultät: | Institut für Wirtschaftsinformatik |
| Studiengang: | Wirtschaftsinformatik |
| Matrikelnummer: | 6922337 |
| Betreuer: | Michael Palk |
| Erstgutachter: | Prof. Dr. Stefan Voß |
| | Institut für Wirtschaftsinformatik |
| Zweitgutachter: | Dr. Kai Brüssau |
| | Institut für Wirtschaftsinformatik |

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# 1 Einleitung

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris. Meanwhile, information technology (IT) has become essential to exchange information between involved inter-organizational actors and across global supply chains more efficiently. Big data can be defined as “data whose size forces us to look beyond the tried-and-true methods that are prevalent at that time.” (Jacobs, 2009, p. 44)

Although a consistent definition of big data has yet to be specified, there is a common understanding that big data is data whose size and complexity forces us to look beyond conventional tools and methods to exploit and utilize it (cf. Jacobs, 2009, p. 44).

According to Jacobs (2009, p. 44), big data can be seen as data whose size $e + p = y$ and complexity forces us to look beyond conventional tool and methods to exploit and utilize it.

- Fink et al. (2005)
- Böse et al. (2000)
- Heilig und Voß (2014)
- Taillard und Voß (2002)
- Davenport und Patil (2012)
- Ropke (2005)
- Heilig und Voß (2015)

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

| | |
|---|---|
| On-demand self-service | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum. |
| Elasticity and scalability | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum. |

**Tabelle 1.1.:** Key characteristics of cloud computing (Armbrust et al., 2010)

# 2 Blockchain 1.0 - Wie Bitcoin funktioniert

Mit Fortschritt im Bereich Kryptographie begann auch das Interesse von Forschern an digitalen Währungen. Das Problem dieser frühen Projekte bestand jedoch darin, dass sie, einen sogenannten *Central Point of Failure*, also eine zentralisierte Schwachstelle besaßen. Beispielsweise könnten die Konten von Nutzern zwar kryptografisch gesichert, jedoch von zentralen Stellen wie Banken verwaltet werden.
Ein wichtiges Problem, welches es mithilfe von Geld zu lösen gilt, ist das sogenannte *Double Spending Problem*. Es muss durch gewisse Mechanismen verhindert werden, dass bösartige Akteure die selben Geldwerte für mehrere Transaktionen verwenden. Bei physischem Geld, also Geldscheinen, Münzen, etc. verhindern komplexe Drucktechniken die Verbreitung von Falschgeld und dadurch das ein Geldschein nur einmal existieren kann, ist dieser nur für eine Transaktion zu verwenden.
Versucht man nun diese Geldwerte gänzlich digital zu verwalten, so liegt die Verantwortung für eine korrekte Beobachtung und Verwaltung bei einer zentralen Stelle wie einer Bank. Diese könnte als Angriffsstelle für Antagonisten dienen und stellt somit eine Gefahr für das System dar.
Dieses Kapitel beschäftigt sich mit der traditionellen Funktionsweise von Geld und wie mithilfe eines dezentralen Systems ein zentraler Fehlerpunkt vermeidet werden kann.

## 2.1 Funktionsweise einer klassischen Transaktion von Geld

Eine Währung, die zum Verwalten und Versenden von monetärem Wert dient, hat drei Probleme zu lösen:

1. Sicherstellung des Wertes, also die Authentizität
2. Garantie dafür, dass die selbe Währung nicht mehr als einmal verwendet werden kann (Double Spending)
3. Zugang zur Währung nur für befugten Besitzer

TODO

## 2.2 Notwendigkeit für Blockchain-Technologie

## 2.3 Theorie der Blockchain-Technologie am Beispiel von Bitcoin

Auch wenn es andere Projekte für dezentrale Währungen wie B-Money und Hashcash gab, begann der Aufschwung digitaler Währungen im Jahr 2008 mit der Veröffentlichung des Bitcoin-Whitepapers *Bitcoin: A Peer to peer Electronic Cash System*. Diese Publikation wurde, von einer bis heute unbekannten Person, unter dem Namen *Satoshi Nakamoto* veröffentlicht und kombinierte Technologien von seiner Vorgänger. Statt einer zentralen Verwaltungsstelle handelt es sich bei Bitcoin um ein dezentrales Peer-to-peer Netzwerk zwischen den Nutzern des Bitcoin-Protokols. Außerdem werden Vermögenswerte nicht durch klassischer Münzen auf einem Konto repräsentiert, sondern durch vergangene Transaktionen in einem dezentralen und öffentlichen Transaktionsbuch, dem sogenannten *Ledger* impliziert. Aufgrund dieser Eigenschaften besteht keine zentrale Angriffsfläche für bösartige Akteure und jeder Akteur im Netzwerk hat Kenntnis über alle Transaktionen. Die folgenden Untersektionen beschäftigen sich mit der Verwaltung und dem Zugang für Nutzer, die Funktionsweise von Transaktionen sowie die Art und Weise, wie die verschiedenen Akteure im Netzwerk zu einem gemeinsamen Konsens kommen.

### 2.3.1 Keys und Adressen

### 2.3.2 Transaktionen

### 2.3.3 Zeitstempel

### 2.3.4 Der Konsensalgorithmus Proof-of-Work

### 2.3.5 Netzwerk

### 2.3.6 Anreize

### 2.3.7 Freimachen von Speicherplatz mittels Hash-Bäumen

### 2.3.8 Verifizierung von Transaktionen

### 2.3.9 Sicherheit und Privatsphäre

### 2.3.10 Angriff auf das Netzwerk

# 3 Blockchain 2.0

## 3.1 Probleme von Bitcoin und Erweiterung der Konzepte durch Ethereum

## 3.2 Theoretische Grundlagen von Ethereum

# 4 Blockchain im Online Advertising

## 4.1 Wie Online Advertising funktioniert

## 4.2 Mögliche Verbesserungen mittels Blockchain-Technologie

## 4.3 Programmierung eines geeigneten Smart Contracts in Solidity

## 4.4 Beantwortung der Forschungsfrage

## 4.5 Blockchain 3.0 - Bestehende Probleme und potenzielle Lösungen

# 5 Zusammenfassung und Ausblick

## 5.1 Zusammenfassung der Kapitel

## 5.2 Diskussion der Ergebnisse

## 5.3 Ausblick

# A Anhang

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Cras semper. Integer sapien nulla, consectetuer a, laoreet et, varius quis, mauris. Nunc pharetra tincidunt massa. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Praesent pellentesque mauris at elit. Aliquam consequat suscipit enim. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nunc sapien. Proin hendrerit diam at quam. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer vulputate semper nunc. Sed dui. Praesent at sem. Integer elit ipsum, placerat vitae, dictum quis, feugiat sit amet, metus.

## A.1 Anhang A

Donec arcu turpis, pretium quis, interdum non, condimentum a, est. Fusce lobortis urna non tellus. Nam leo dui, malesuada non, tempus placerat, congue eget, pede. Mauris porttitor risus quis tortor molestie vehicula. Curabitur tincidunt. In malesuada congue nisi. Nullam et nulla. Curabitur porttitor. Ut molestie sagittis felis. Sed urna libero, ultricies quis, laoreet eget, congue id, metus. Proin ac lorem cursus mauris auctor laoreet. Donec justo. Etiam nunc sem, dapibus sit amet, euismod a, molestie sit amet, mi.

Morbi sollicitudin consequat magna. Vivamus dictum. Nulla non quam. Nam sem tellus, aliquam sed, hendrerit nec, imperdiet ut, augue. Aliquam erat volutpat. Vivamus non ligula sit amet lorem accumsan viverra. Cras mattis libero et ante. Cras massa. Donec fringilla, metus vitae semper condimentum, dolor dui fringilla arcu, et mattis nulla dui vel lectus. Nunc mauris magna, tristique eu, rutrum at, facilisis eu, odio. Nullam congue magna non nisi. Suspendisse viverra, massa non pellentesque scelerisque, risus elit

Hier kommt ein Listing A.1.

```
1  <?xml version='1.0' encoding='UTF-8'>
2  <SOAP-ENV:Envelope
3    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
4    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
6    xmlns:ns1="http://localhost/wsdl/HalloWeltService.wsdl">
7
8    <SOAP-ENV:Body>
9      <ns1:gruss>
10       <name xsi:type="xsd:string">
```

```
11          Michael
12        </name>
13      </ns1:gruss>
14    </SOAP-ENV:Body>
15
16 </SOAP-ENV:Envelope>
```

**Listing A.1:** SOAP Anfrage an einen HalloWelt-Web-Service

bibendum dolor, vitae ultrices lorem neque et erat. Nullam tortor ante, venenatis et, aliquet ac, ornare id, massa. Vivamus urna augue, posuere vitae, sagittis id, porttitor at, arcu. Praesent pharetra rutrum neque. Maecenas tempor ultrices felis. Nulla facilisi. In sed elit aliquet neque malesuada blandit. Nam tempus imperdiet eros. Mauris tincidunt diam eu erat. Phasellus iaculis blandit leo. Nunc augue. Donec dignissim accumsan pede. Ut consequat, eros id accumsan placerat, mi justo ullamcorper pede, id lacinia augue nisi non nibh. Vestibulum eget arcu. Cras pretium, dui eu gravida varius, lectus neque accumsan ligula, eu sodales magna lectus ut nisi. Aliquam vel ante. Ut suscipit porta augue. Suspendisse pellentesque faucibus nisl. Nulla magna tortor, cursus quis, varius quis, hendrerit ut, neque.

# Literaturverzeichnis

Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al. (2010). A view of cloud computing. *Communications of the ACM 53*(4), 50–58.

Böse, J., T. Reiners, D. Steenken, S. Voß (2000). Vehicle dispatching at seaport container terminals using evolutionary algorithms. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS)*. IEEE, Maui, HI, USA, 1–10.

Davenport, T. H., D. J. Patil (2012). Data scientist: The sexiest job of the 21st century. https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/. Letzter Zugriff am 09.12.2015.

Fink, A., G. Schneidereit, S. Voß (2005). *Grundlagen der Wirtschaftsinformatik* (2. Aufl.). Physica, Heidelberg.

Heilig, L., S. Voß (2014). A scientometric analysis of cloud computing literature. *IEEE Transactions on Cloud Computing 2*(3), 266–278.

Heilig, L., S. Voß (2015). Inter-terminal transportation: An annotated bibliography and research agenda. Working paper, Institute of Information Systems, University of Hamburg.

Jacobs, A. (2009). The pathologies of big data. *Communications of the ACM 52*(8), 36–44.

Ropke, S. (2005). *Heuristic and exact algorithms for vehicle routing problems*. Doktorarbeit, University of Copenhagen.

Taillard, E. D., S. Voß (2002). POPMUSIC – Partial Optimization Metaheuristic under Special Intensification Conditions. In Celso C. Ribeiro, Pierre Hansen (Hrsg.), *Essays and Surveys in Metaheuristics*, 613–629. Kluwer, New York, NY, USA.

# Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit im Studiengang Wirtschaftsinformatik selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet-Quellen – benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht. Ich versichere weiterhin, dass ich die Arbeit vorher nicht in einem anderen Prüfungsverfahren eingereicht habe und die eingereichte schriftliche Fassung der auf dem elektronischen Speichermedium entspricht.

Hamburg, den _____ Unterschrift: _____