Hochschule Esslingen
University of Applied Sciences

Forschungsarbeit

Digital Rights Management und Rechteübertragung

Konzept für die Umsetzung und Kontrolle der rechtmäßigen Nutzung digitaler Medien auf Basis der Technologie Blockchain.

Fakultät Informatik
der Hochschule Esslingen

vorgelegt von

Fabian Schirmer
Matrikelnummer: 759951

Abgabetermin: DD.MM.JJJJ

Betreuer:	Prof. Dr. Peter Väterlein
Berater:	Rechtsanwalt Dr. Sascha Theißen (Fachanwalt für Urheber- und It-Recht)

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Abschlussarbeit selbstständig und nur unter Verwendung der von mir angegebenen Quellen und Hilfsmittel verfasst zu haben. Sowohl inhaltlich als auch wörtlich entnommene Inhalte wurden als solche kenntlich gemacht. Die Arbeit hat in dieser oder vergleichbarer Form noch keinem anderem Prüfungsgremium vorgelegen.

Datum: _____ Unterschrift: _____

Danksagung

Mein besonderer Dank geht an Professor Dr. Peter Väterlein sowie Dr. Sascha Theißen für die technische Unterstützung, womit Sie mir bei der Konzeption und Durchführung dieser Arbeit wesentlich geholfen haben. Die Kooperation war nicht nur wissenschaftlich, sondern auch menschlich sehr fördernd für diese Arbeit.

Zusammenfassung

Abstract

Inhaltsverzeichnis

Abkürzungsverzeichnis

KDE K Desktop Environment

Bash Bourne again shell

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Der Wandel vom Industriezeitalter zum Digitalzeitalter schreitet immer schneller voran. Dies macht sich nicht nur im geschäftlichen sondern auch im privaten Umfeld bemerkbar. Digitale Medien gewinnen mehr und mehr die Oberhand. Dies ruft gleichzeitig kriminelle Handlungen auf den Plan. Diese Arbeit versucht einen Lösungsweg für diese Problematik zu arbeiten und eine sichere Methode vorzustellen, welche Langfristig eine Sicherheit bietet. So lässt sich durch Studium dieser Arbeit

1.1 Motivation

Derzeit befinden sich auf dem Markt sehr viele proprietäre Systeme, welche DRM (Digital Rights Management) zum Schutz digitaler Medien anbieten. Allerdings sind solche Anwendungen zum einen sehr einschränkend für den Benutzer. Das beutet entweder die Beschränkung auf eine bestimmte Hardware oder die Einschränkung des Nutzungsverhaltens.

1.2 Ziel der Arbeit

Ziel dieser Arbeit ist es ein Konzept aufzuzeigen welches einen Mehrwert für die Verlage und für den jeweiligen Nutzer bietet. Dabei werden die Stichworte Sicherheit und gleichzeitige Anonymität auf Basis des juristischen Kontextes beachtet.

1.3 Überblick

2 Vorbetrachtungen und Grundlagen

In den nachfolgenden Punkten erfolgt eine Definition, Einordnung und interdisziplinäre Betrachtung der digitalen Rechteverwaltung. Im Kontext dazu werden das gesellschaftliche und juristische Umfeld näher beleuchtet.

2.1 Begriffsdefinition Digital Rights Management

Bevor mit der eigentlichen Betrachtung von Digital Rights Management(DRM) begonnen wird, ist eine einleitende Definition zum besseren Verständnis aufgeführt. Das Konzept DRM umfasst sogenannte Nutzungsregeln für ein digitales Objekt. Dabei umfasst der Begriff digitales Objekt alle möglichen digitalen Informationsmedien wie beispielsweise Bilder, eBooks usw. Die Nutzungsparameter umfassen dabei folgende Einschränkungen:

- *Wer* ist berechtigt die digitalen Inhalte zu nutzen?
- *Wann* und *Wo* werden die digitalen Inhalte genutzt?
- *Wie* wird das digitale Medium benutzt?

Dabei beinhaltet *Wer* den Nutzungsberechtigten für das digitale Objekt, *Wann* den Nutzungszeitraum(zeitlich begrenzte oder unbegrenzte Leihe) und *Wo* definiert das autorisierte Abspielmedium. Das *Wie* weißt beispielsweise Schreibrechte oder ausschließlich Leserechte dem Berechtigten zu. [Willms Buhse, 2008, S.227]
Neben dem Aufstellen der spezifischen Nutzungsregeln ist aber auch die Überwachung und Einhaltung dieser Parameter ein elementarer Bestandteil solcher Systeme. Dies wird zumeist von proprietärer Software übernommen, die die Einhaltung der Nutzungsbedingungen für das digitale Objekt gewährleistet.

2.2 Aufbau von DRM Systemen

Um ein besseres Verständnis über die Abläufe innerhalb eines DRM-basierten Systems zu bekommen, wird im Folgenden der grundsätzliche Aufbau solcher Systeme erläutert.

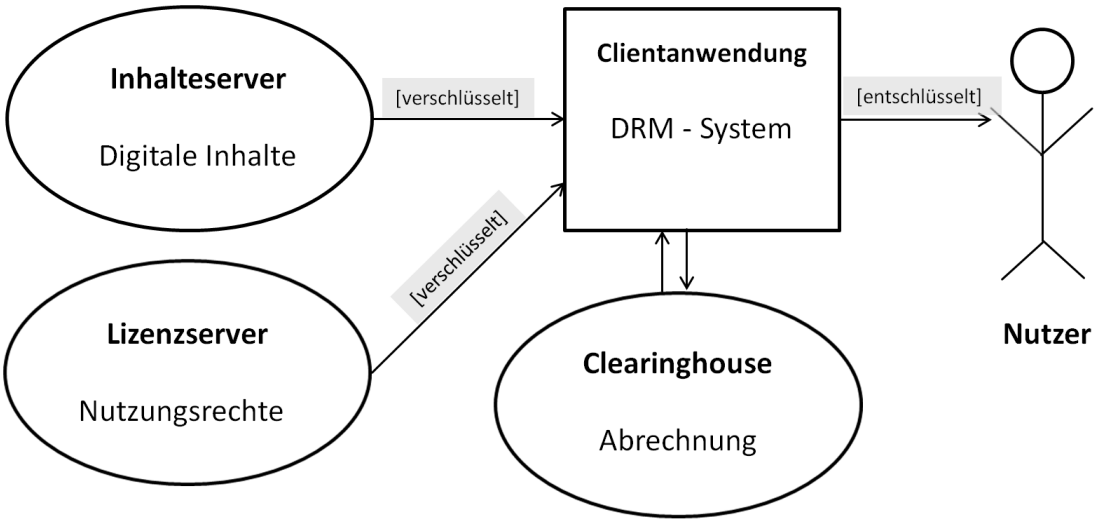

Abbildung 2.1: DRM Ablaufschema

Dieser Prozess, welcher in Abbildung 2.1 zu sehen ist, gliedert sich in drei Kernelemente. Um den architektonischen Aufbau derzeitiger Systeme zu verstehen, werden diese Kernelemente kurz vorgestellt.

- **Inhalteserver**

  Der Inhalteserver stellt das digitale Objekt in verschlüsselter Form zur Verfügung.

- **Lizenzserver**

  Der Lizenzserver stellt die Nutzungsregeln für das digitale Objekt in verschlüsselter Form zur Verfügung. Diese können in feingranular unterteilt werden. Nähre Informationen sind unter 2.8 zu finden.

- **Clientanwendung**

  Die Clientanwendung ist ein proprietäres System, welches das chiffrierte digitale Objekt und die jeweiligen Nutzungsrechte verarbeitet. Basierend auf den Nutzungsregeln wird das entschlüsselte digitale Objekt dem Anwender zur Verfügung gestellt. Jeglicher Fehlgebrauch, der nicht auf den Nutzungsregeln basiert, wird unterbunden.

Um die Digital Rights Management Systeme auch aus kommerzieller Sicht zu komplementieren wird eine sogenanntes *Clearinghouse* in das Gesamtkonstrukt eingebettet. Dieses

übernimmt den Zahlungsvorgang. Dabei werden nachträgliche Erweiterung im Nutzungsrecht ebenfalls über diese Stelle abgewickelt [Becker et al., 2003, S.151]. Nähere Informationen zum ökonomischen Standpunkt sind unter 2.8 aufgelistet.

!!Aüßere Form + Zitatquelle überprüfen
Neben der allgemeinen Definition haben sich zwei spezialisierte Konzepte der Digitalen Rechteverwaltung herausgebildet, die im nachfolgenden kurz vorgestellt werden.

2.3 Hard Weight DRM

Der zuvor geschilderte Aufbau eines DRM-Systems wird auch als *Hard DRM* bezeichnet. Dieses umfasst alle proprietären Systeme, die auf eine strikte Einhaltung der Nutzungsrechte beharren. Das digitale Objekt kann nur in der Art und Weise genutzt werden, wie es in den dazugehörigen Nutzungsregeln hinterlegt ist. Somit werden nur autorisierte Benutzer Zugang zum digitalen Medium gewährt. Gleichzeitig wird eine Autorisierung durchgeführt, die den Aktionsumfang für den Benutzer festlegt und somit entsprechend einschränkt. Möchte man den Umfang der Aktionen erweitern, kann dies durch Kauf zusätzlicher Nutzungsregeln initiiert werden [Regner et al., 2009, S.335].
Starke Einschränkungen rufen immer wieder illegale Machenschaften in den Fokus. Aufgrund dessen haben sich Industrie und Wissenschaft mit Alternativlösungen auseinandergesetzt.

2.4 Light Weight DRM

Der Gedanke hinter der sogenannten *leichten digitalen Rechteverwaltung* ist ein Verzicht das Beharren auf Einhaltung der Nutzungsbestimmungen. Somit werden dem Endverbraucher mehr Freiheiten gewährt, was zu einer größeren Akzeptanz führt.
Jedes erworbene digitale Gut wird mit einer digitalen Signatur dem Benutzer zugeordnet. Die digitale Signatur ist wie eine Unterschrift in der analogen Welt anzusehen. Dieses Verfahren verursacht keinerlei Einschränkungen bei der Nutzung. Wird allerdings gegen die Nutzungsregeln verstoßen, so kann eindeutig nachgewiesen werden, wer gegen diese verstoßen hat. Mit diesem Wissen können im Nachhinein strafrechtliche Verfolgungen eingeleitet werden.

Um für die Konsumenten einen Anreiz zu schaffen, dass jeweilige digitale Produkt mittels Superdistribution[1] weiterzuverbreiten, ist das *PotatoSystem* entwickelt worden. Dieses begünstigt
[Arnold Picot, 2005, S. 90 ff.]

2.5 Anforderungen an DRM

2.5.1 Authentifikaiton

2.5.2 Autorisierung

2.6 Juristische Betrachtung

Digital Rights Management Systeme bewegen sich in einen schwierigen Terrain. Nicht zuletzt das es sich bei digitalen Objekten um immaterielle, nicht greifbare Gegenstände handelt.

2.6.1 Recht auf Löschung der Daten

2.6.2 Recht auf Privatkopie

2.6.3 Datenschutzgrundverordnung

2.6.4 Urheberrecht

2.7 Gesellschaftliche Betrachtung

2.8 Ökonomische Betrachtung

1. passive Nutzungsbestimmungen
    - Zeitraumbegrenzung
    - Anzahl der Nutzungen
    - Länderbeschränkung

[1] Verbreitung von chiffrierten digitalen Objekten unter den Benutzern über das Internet, Bluetooth oder sonstige standardisierte Übertragungswege [Yen et al., 2012]

2. aktive Nutzungbestimmungen
    - Leserechte
    - bestimmte Anzahl von Druckkopien
    - Schreibrechte
3. Nutzungsberechtigte
    - eindeutige Benutzerzuweisung
    - eindeutige Gerätezuweisung

https://onlinelibrary.wiley.com/doi/pdf/10.1002/spe.2479 Eventuell eigene Grafik erstellen

2.9 Bestehende Probleme

Vorangegange Betrachtungen haben das generelle Bild der digitalen Rechteverwaltung zum einen klar definiert. Zum anderen wurde eine gesellschaftliche und juristische Einordnung vorgestellt, die das Gesamtbild abrundet.

3 Stand der Technik

3.1 DRM Architekur

3.2 Verschlüsselung

3.3 Digitale Wasserzeichen

3.4 Trusted Computing

3.5 Rechtedefinitionssprachen

4 Konzept auf Basis der Technologie Blockchain

4.1 Themenbezogene Veröffentlichungen

4.2 Funktionsweise

5 Ergebnisse

6 Diskussion

6.1 Zusammenfassende Bewertung

6.2 Ausblick

Literaturverzeichnis

[Arnold Picot, 2005] Arnold Picot, H. T., editor (2005). *Distribution und Schutz digitaler Medien durch Digital Rights Management*. Springer-Verlag Berlin Heidelberg.

[Becker et al., 2003] Becker, B., Buhse, W., Günnewig, D., and Rump, N., editors (2003). *Digital Rights Management*. Springer Verlag.

[Regner et al., 2009] Regner, T., Barria, J. A., V.Pitt, J., and Neville, B. (2009). An artist life cycle model for digital media content: Strategies for the Light Web and the Dark Web. In *Electronic Commerce Research and Applications*.

[Willms Buhse, 2008] Willms Buhse, D. G. (2008). *Ökonomie der Musikindustrie*. Gabler.

[Yen et al., 2012] Yen, C.-T., Liaw, H.-T., and Lo, N.-W. (2012). Digital rights management system with user privacy, usage transparency, and superdistribution support. *International Journal of Communicatio Systems*.