Bachelorarbeit

im Studiengang
Wirtschaftsinformatik und digitale Medien

Ein sicheres Peer-to-Peer-Instant-Messaging-Protokoll unter Berücksichtigung von Blockchain-Technologie

vorgelegt von

Nicole Sauer

an der Hochschule der Medien Stuttgart
am 29.01.2024
zur Erlangung des akademischen Grades eines
Bachelor of Science

Erstprüfer	Prof. Dr. Peter Thies
Zweitprüfer	Prof. Dr. Stephan Wilczek

Ehrenwörtliche Erklärung

Hiermit versichere ich, Nicole Sauer, ehrenwörtlich, dass ich die vorliegende Bachelorarbeit mit dem Titel: „Ein sicheres Peer-to-Peer-Instant-Messaging-Protokoll unter Berücksichtigung von Blockchain-Technologie“ selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Ebenso sind alle Stellen, die mit Hilfe eines KI-basierten Schreibwerkzeugs erstellt oder überarbeitet wurden, kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Ich habe die Bedeutung der ehrenwörtlichen Versicherung und die prüfungsrechtlichen Folgen (§ 24 Abs. 2 Bachelor-SPO), der HdM einer unrichtigen oder unvollständigen ehrenwörtlichen Versicherung zur Kenntnis genommen.

Leutenbach, den 29.01.2024 

Ort, Datum	Unterschrift

Inhaltsverzeichnis

Kapitel 1

Einleitung

In den letzten Jahren hat sich die digitale Kommunikation signifikant gewandelt. 2013 war das Short Message System (SMS) noch dominierend, doch in den darauf folgenden Jahren verlagerte sich der Fokus deutlich hin zum Mobile Instant Messaging. Die Nutzung von Instant Messaging unter der deutschen Bevölkerung stieg von etwa 24% im Jahr 2013 auf beeindruckende 73% im Jahr 2017 (Nier 2017).
In der heutigen digitalen Welt, geprägt von ständiger Vernetzung und dem Bedarf an schnellem und sicheren Informationsaustausch, stehen sicheres Instant Messaging und die Blockchain-Technologie im Zentrum eines tiefgreifenden Wandels. Während Instant Messaging die Art und Weise revolutioniert hat, wie Menschen miteinander kommunizieren, indem es Echtzeitkommunikation über Text, Bilder und Videos ermöglicht, hat die Blockchain-Technologie in den Bereichen Finanzen, Datensicherheit und digitale Transaktionen eine disruptive Veränderung eingeleitet. Interessanterweise sind diese beiden Konzepte keineswegs voneinander isoliert, sondern vielmehr eng miteinander verknüpft.

Instant Messaging-Plattformen sehen sich mit der Herausforderung konfrontiert, die Privatsphäre und Sicherheit ihrer Nutzer zu gewährleisten, insbesondere angesichts wachsender Bedenken hinsichtlich Datenschutz und Sicherheit. Hier kommt die Blockchain ins Spiel. Ihre dezentrale Natur und die Fähigkeit, Transaktionen und Daten in einer fälschungssicheren Umgebung zu speichern, bietet eine vielversprechende Lösung. Blockchain kann dazu beitragen, die Vertraulichkeit von Instant Messaging-Nachrichten und die Identität der Nutzer zu schützen, da sie

eine manipulationssichere Aufzeichnung aller Transaktionen ermöglicht.

Darüber hinaus hat die Blockchain das Potenzial, die Integrität und Authentizität von Dateien und Dokumenten in Instant Messaging-Plattformen sicherzustellen. Dies ist von entscheidender Bedeutung, insbesondere in geschäftlichen Kontexten, in denen Verträge und wichtige Informationen ausgetauscht werden. Die Integration von Blockchain in Instant Messaging-Plattformen verspricht somit eine sicherere und vertrauenswürdigere Kommunikation.

In dieser Wechselwirkung zwischen sicheren Instant Messaging-Plattformen und Blockchain-Technologie zeigt sich, wie diese beiden Konzepte gemeinsam dazu beitragen, die Sicherheit und Integrität von digitalen Kommunikationsprozessen zu gewährleisten. Es ist ein aufregendes Zusammenspiel, das die Art und Weise, wie wir kommunizieren und Geschäfte tätigen, nachhaltig beeinflusst und in Zukunft noch weiterentwickelt werden könnte.

Sicheres Instant Messaging und Blockchain sind zwei Schlüsselkonzepte, die in der heutigen digitalen Ära eine herausragende Rolle spielen. Während Instant Messaging die Art und Weise verändert hat, wie Menschen in Echtzeit miteinander kommunizieren, hat Blockchain eine Revolution in der Art und Weise ausgelöst, wie Transaktionen und Datenmanagement in einer dezentralen, sicheren Umgebung stattfinden. Diese beiden Technologien sind in vielerlei Hinsicht miteinander verknüpft, da sie gemeinsam das Potenzial bieten, die Sicherheit, Integrität und Transparenz in der digitalen Kommunikation und im Datenaustausch zu gewährleisten. In diesem Zusammenhang ist es entscheidend, das Zusammenspiel von sicheren Instant-Messaging-Plattformen und der Blockchain-Technologie zu betrachten, um ein umfassendes Verständnis davon zu erlangen, wie sie unsere moderne Kommunikationslandschaft und Geschäftswelt prägen

Kapitel 2

Grundlagen

2.1 Instant Messaging

Instant Messaging ist heute relevanter als je zuvor...

2.2 Blockchain-Technologie

Die Blockchain-Technologie ist...

2.3 Peer-to-Peer-Technologie

Unter der Peer-to-Peer-Technologie versteht man...

2.4 Sicherheit im Instant Messaging

Folgende Sicherheitsaspekte sollte im Instant Messaging betrachtet werden...

2.5 Existierende IM-Protokolle

Es gibt bereits diverse IM-Protokolle, die P2P verwenden, aber...

Kapitel 3

Anforderungen

Hier stehen die Anforderungen

Kapitel 4

Entwurf und Architektur

4.1 Protokolldesign und -struktur

Das Protokoll ist wie folgt strukturiert...

4.1.1 Grundlagen des Protokolls

Das Protokoll funktioniert auf der Grundlage eines vollständig dezentralen Peer-to-Peer-Modells, das es Benutzern ermöglicht, direkt miteinander zu kommunizieren, ohne Vermittler. Nachrichten und Daten werden direkt zwischen Benutzern ausgetauscht und nutzen eine Ende-zu-Ende-Verschlüsselung zur Sicherheit.

4.1.2 Verbindung und Identität

Benutzer können andere Peers in einem verteilten Netzwerk entdecken und sich mit ihnen verbinden. Dies kann verteilte Hash-Tabellen (DHTs) oder andere Mechanismen zur Peer-Erkennung umfassen. Benutzer werden durch eindeutige öffentliche Schlüssel identifiziert, und Benutzerprofile können zusätzliche Informationen wie Benutzernamen, Avatare und Status enthalten.

4.1.3 Nachrichten und Daten

Benutzer können ausschließlich Textnachrichten miteinander austauschen. Diese Nachrichten können an einzelne Peers gesendet werden. Die gesamte Kommuni-

kation ist mit starken Verschlüsselungsalgorithmen verschlüsselt, um Privatsphäre und Sicherheit zu gewährleisten.

4.1.4 Nachrichtenverlauf

Benutzer haben die Möglichkeit, ihren Nachrichtenverlauf lokal zu speichern. Der Nachrichtenverlauf ist ebenfalls verschlüsselt, um die Sicherheit zu gewährleisten.

4.1.5 Sicherheit

Alle Nachrichten sind mit öffentlichen Schlüsseln verschlüsselt, um sicherzustellen, dass nur der beabsichtigte Empfänger die Nachrichten entschlüsseln und lesen kann. Ein sicheres Verfahren für den Schlüsselaustausch und die Schlüsselverwaltung wird implementiert, um gegen Abhören und Man-in-the-Middle-Angriffe zu schützen.

4.2 Technologien und Tools

Für die Umsetzung dieses Designs wurden diese Technologien verwendet.

4.3 Integration von Blockchain in das Protokoll

Bei der Auswahl der Blockchain fiel die Entscheidung auf Ethereum.

Kapitel 5

Sicherheit ???

Wir das überhaupt benötigt?

Kapitel 6

Evaluierung

Hier ist die Evaluierung.

Kapitel 7

Diskussion

Hier ist die Diskussion.

Kapitel 8

Schlussfolgerung und Ausblick

Hier ist die Schlussfolgerung.

Webseiten

Nier, Hedda (2017). *Wie sich die digitale Kommunikation verändert hat*. Zugriff am 30.10.2023. URL: https://de.statista.com/infografik/11426/wie-sich-die-digitale-kommunikation-veraendert-hat/.