h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Hochschule Darmstadt

– Fachbereich Informatik–

Untersuchung von Hyperledger Fabric für Blockchain-Technologien und dessen Anwendung für eine Kryptowährung hinsichtlich Privatheit und Performance

Abschlussarbeit zur Erlangung des akademischen Grades

Master of Science (M.Sc).

vorgelegt von

Bernd Nötscher

Referent	:	Prof. Dr. Alois Schütte
Korreferent	:	Prof. Dr.-Ing. Michael Bredel

ERKLÄRUNG

Ich versichere hiermit, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Darmstadt, 25. August 2018

Bernd Nötscher

ABSTRACT

Private and permissioned blockchains offer new possibilities for applications in the B2B environment and have recently been the focus of attention.

This thesis examines and evaluates the individual components of Hyperledger Fabric, an open source framework for private and permissioned blockchains.

A concept of a crypto currency and its implementation with Hyperledger Fabric is presented as a practical application. In addition to the Java client, the configuration and setup of the peer-to-peer network using Docker and AWS is explained. Furthermore, this paper describes how the conventional programming language Golang is used for the smart contracts to implement a crypto currency consisting of several blockchains.

This paper shows that this crypto currency achieves a performance of at least 18 transactions per second, with minimal latency and immediate finality, using a consensus based on majority votings. At the same time, privacy (e.g. non-traceability) is guaranteed through the use of encryption methods (such as AES and RSA), pseudonyms and data separation.

In the end, the known crypto currencies Bitcoin and Monero are analyzed and compared in terms of performance, privacy and non-traceability.

Keywords:
Distributed Ledger Technology, Blockchain Technology, Hyperledger Fabric, Smart contracts, Chaincode, Cryptocurrency, Private Blockchains

ZUSAMMENFASSUNG

Private und zugangsbeschränkte Blockchains bieten neue Möglichkeiten für Anwendungen im B2B-Umfeld und stehen entsprechend im Fokus der letzten Zeit.

Diese Thesis untersucht und bewertet die einzelnen Komponenten von Hyperledger Fabric, einem Open-Source-Framework für private und zugangsbeschränkte Blockchains.

Als praktische Anwendung wird ein Konzept einer Kryptowährung und die dazugehörige Implementierung mit Hyperledger Fabric vorgestellt. Dabei wird neben dem Java-Client die Konfiguration und Inbetriebnahme des Peer-to-Peer-Netzwerks durch Verwendung von Docker als auch AWS erläutert. Weiterhin beschreibt diese Arbeit wie die konventionelle Programmiersprache Golang für die intelligenten Verträge verwendet wird um eine Kryptowährung bestehend aus mehreren Blockchains zu implementieren.

Mit dieser Arbeit wird gezeigt, dass diese Kryptowährung mit Hilfe eines auf Mehrheitsentscheidungen basierenden Konsens eine Performance von mindestens 18 Transaktionen pro Sekunde erreicht, bei minimaler Latenz und sofortiger Finalität. Gleichzeitig wird die Privatheit (wie z. B. die Nichtnachverfolgbarkeit) durch die Anwendung von Verschlüsselungsverfahren (wie AES und RSA), Pseudonymen und Datenseparation gewährleistet.

Am Ende werden die bekannten Kryptowährungen Bitcoin und Monero analysiert und mit diesen ein Vergleich hinsichtlich Performance, Privatheit und Nichtnachverfolgbarkeit vollzogen.

Schlüsselwörter:
Distributed Ledger Technologie, Blockchain Technologie, Hyperledger Fabric, Smart contracts, Chaincode, Kryptowährungen, Private Blockchains, Intelligente Verträge

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LISTE DER QUELLLTEXTE

Teil I

THESIS