Westfälische Hochschule

Wissen.
Was praktisch zählt.

Blockchain –

Methode zur Zertifizierung von Forschungsdaten

Autoren: Kevin Wittek, Dominik Krakaus, Sebastian Posth, Norbert Pohlmann

Bereits 2013 wurde eine Bitcoin-basierte Implementierung eines Proof-of-Existence (PoE)-Dienstes für digitale Dokumente entwickelt und veröffentlicht. Sie verfolgt den Ansatz, einen kryptographischen Hash eines Dokuments auf einem öffentlichen Ledger zu speichern. Dieser öffentliche Notarisierungsdienst beweist die Existenz eines Dokuments zu einem bestimmten Zeitpunkt, ohne den Inhalt des Dokuments selbst preiszugeben. Ein ähnlicher Ansatz wurde für eine sichere und manipulationsresistente Speicherung klinischer Studiendaten vorgeschlagen, wobei insbesondere auf das Potenzial zur Verbesserung der allgemeinen Qualität der klinischen Forschung im Hinblick auf Rückverfolgbarkeit und sichere Automatisierung hingewiesen wurde.
Darüber hinaus wurden Blockchain und DLT-basierte Ansätze diskutiert, die Probleme im Bereich des geistigen Eigentums und des Urheberrechts adressieren: z. B. für ein vertrauenswürdiges System zur Einreichung von Manuskripten mit Zeitstempel für Peer-Reviews und eine auditierbare Plattform für kollaboratives Design-Thinking und offene Innovation.
Basierend auf diesen Erkenntnissen und den Anforderungen der wissenschaftlichen Gemeinschaft haben wir eine Softwarebibliothek für die Integration der MATLAB-Computing-Umgebung mit der auf akademische Zwecke ausgerichteten *bloxberg*-Blockchain-Infrastruktur entwickelt, die eine nahtlose Einbindung der Existenznachweise für Forschungsrohdaten in bestehende wissenschaftliche Prozesse ermöglicht.

bloxberg
Die *bloxberg*-Infrastruktur ist eine globale Blockchain, die von einem internationalen Konsortium wissenschaftlicher Organisationen verwaltet und betrieben wird. Ziel der Infrastruktur ist es, der akademischen Gemeinschaft eine öffentliche Blockchain als Dienstleistung anzubieten und dadurch die Zusammenarbeit der Wissenschaftler und Institute zu fördern.
Im Vergleich zu anderen bekannten, öffentlichen Blockchain-Netzwerken wie Bitcoin und Ethereum, die auf Proof-of-Work (PoW) als Consensus-Algorithmus basieren, verwendet die *bloxberg*-Blockchain Proof-of-Authority (PoA) mit Authority Round (Aura) als Consensus-Algorithmus. Dieser Algorithmus reduziert den Verbrauch von Energie für den Betrieb einer Blockchain auf ein Minimum und erhöht den potenziellen Durchsatz von Transaktionen bei gleichzeitiger Aufrechterhaltung der Dezentralisierung durch die Verteilung von Block-Signaturen zwischen den teilnehmenden wissenschaftlichen Organisationen. Da es sich bei den validierenden Knoten im Netzwerk um bekannte Entitäten handelt, können außerdem spezifische Rechen- und Netzwerkanforderungen von den beteiligten Knoten erfüllt werden. Diese Eigenschaft gewährleistet Skalierbarkeit und einen höheren Grad an Effizienz im Vergleich zu PoW-basierten Blockchains, während gleichzeitig das Konzept einer dezentralen und verteilten Vertrauensarchitektur durch das Konsortium internationaler Forschungsorganisationen gewährleistet wird. Diese Aspekte machen das bloxberg-Netzwerk zu einer idealen Infrastruktur, auf der wissenschaftlich fokussierte Blockchain-Anwendungen aufbauen können. Eine dieser bereits existierenden Anwendungen ist die Certify-dApp.

Certify-dApp
Der *Certify-dApp* ist eine prototypische decentralized application (dApp), die im *bloxberg*-Netzwerk betrieben wird. Sie kann verwendet werden, um die Existenz einer beliebigen Datei, z. B. mit generischen Forschungsdaten, zu einem bestimmten Zeitpunkt zu verifizieren, ohne den Inhalt der Datei selbst preiszugeben.
Zu diesem Zweck wird der SHA-256-Hash der Datei zusammen mit zusätzlichen Metadaten in einer Transaktion im *bloxberg*-Netzwerk veröffentlicht – das deutsche Bundesamt für Sicherheit in der Informationstechnik attestiert diesem Hash eine starke kryptographische Sicherheit. Der Zeitstempel der Transaktion fungiert als öffentlicher Datensatz, der die Existenz der zertifizierten Daten zu diesem Zeitpunkt beweist. Es ist dadurch möglich, die Existenz einer Datei zu einem späteren Zeitpunkt zu überprüfen, indem man den Zeitstempel der ersten Transaktion, die ihren SHA-256-Hash enthält, im *bloxberg*-Netzwerk nachschlägt.
Die *Certify-dApp* kann von Nutzer/-innen als echte *dApp* in Verbindung mit einer Wallet-Software (z. B. MetaMask) verwendet werden. Darüber hinaus ist es Nutzer/-innen aber auch möglich, mit der Anwendung ohne Wallet online zu interagieren. Ein Zugang wird durch eine Webanwendung möglich, die als Proxy oder Vermittler gegenüber dem *bloxberg*-Netzwerk agiert und Transaktionen über eine kustodiale Wallet veröffentlicht.
Darüber hinaus sind Verbesserungen der Zugänglichkeit und des Benutzererlebnisses durch die Entwicklung von Client-Software und Integrationen möglich. Beispielhaft ist z. B. die Single-Button-Integration der Max Planck Digital Library in ihre bestehende interne Cloud-Speicherlösung KEEPER. Die Einbindung anderer wissenschaftlicher Cloud-Lösungen, wie z. B. Sciebo, ist theoretisch ebenfalls möglich.

Nächste Schritte
Aktuell ist es lediglich möglich, einzelne Forschungsdaten als atomare Einheit zu zertifizieren. In Zukunft soll das gesamte Potenzial der Anwendung dadurch erschlossen werden, den wissenschaftlichen Prozess als Ganzes über seine gesamte Lebensdauer zu zertifizieren. Dieses Konzept könnte neben den Zwischenergebnissen und endgültigen Forschungsdaten auch Artefakte wie z.B. Versuchspläne und -methoden, technische Versuchsaufbauten und verwendete Hardware (idealerweise in Form von cyber-physikalischen Systemen), Quellcode und verwendete Software, Versuchspersonen (z. B. digitale Identitäten von Menschen und Tieren) und Versuchsleiter umfassen.
Aktuell bemüht sich die bloxberg-Community bereits in Form von bloxberg-Improvement Proposals (BLIPs), die Herausforderung der Zertifizierung eines mehrdimensionalen wissenschaftlichen Prozesses in Angriff zu nehmen. BLIPs orientieren sich an etablierten Community-getriebene Projekte zur Standardisierung von Software, wie Ethereum Improvement Proposals (EIP) und JDK Enhancement Proposals (JEP) .
Die vollständigen Ergebnisse dieses Forschungsvorhabens,an dem Wissenschaftler der Ruhr-Universität Bochum und des Max Planck Digital Library beteiligt waren, sind im akademischen Paper “Integrating bloxberg's Proof of Existence Service With MATLAB” im Detail dokumentiert, das frei zugänglich im ‘Frontiers in Blockchain’-Journal erschienen ist.
Der Zugang zum *bloxberg*-Netzwerk steht interessierten Forschern und Firmen jederzeit über den vom Institut für Internet-Sicherheit betriebenen Blockchain-Knoten zur Verfügung. Bei Interesse bitten wir um eine Kontaktaufnahme mit Kevin Wittek, Leiter des Blockchain-Labs im Institut für Internet-Sicherheit (wittek@internet-sicherheit.de).

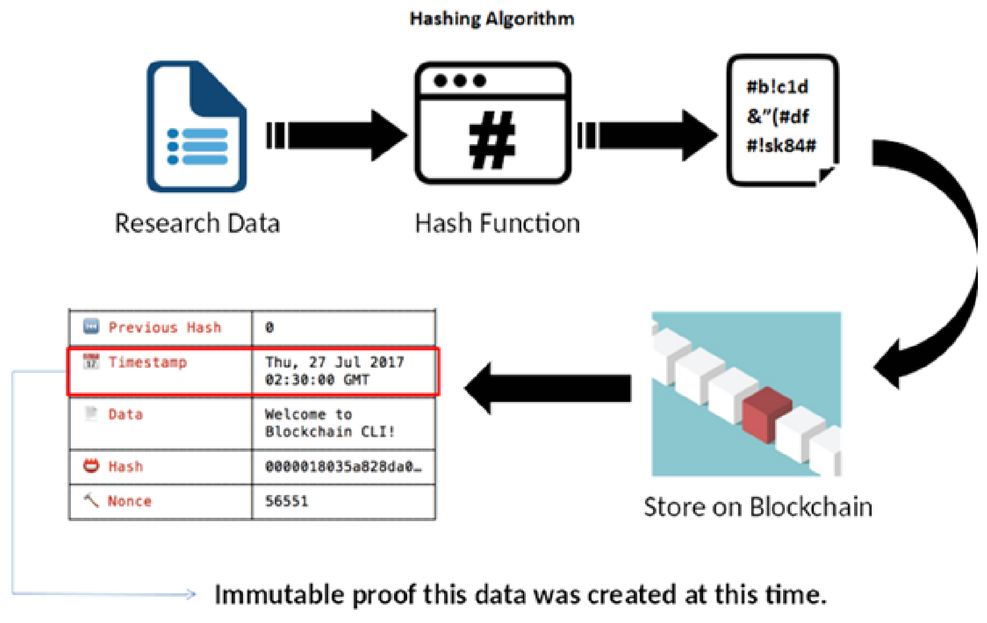

Abb 1: Proof-of-Existence Prozess

Kontakt

Prof. Dr. (TU NN) Norbert Pohlmann
Tel. +49 209 9596-515
E-Mail: norbert.pohlmann@w-hs.de

Kevin Wittek
Tel. +49 209 9596-696
E-Mail: wittek@internet-sicherheit.de

Institut für Internet-Sicherheit – if(is)
E-Mail: information@internet-sicherheit.de
Tel.: +49 209 9596-515
www.internet-sicherheit.de

Westfälische Hochschule
Neidenburger Straße 43
45897 Gelsenkirchen
www.w-hs.de

if(is) internet-sicherheit