Datenschutz und Datensicherheit

Die Nutzung der Blockchain-Technologie bietet zahlreiche Vorteile in Bezug auf die Datensicherheit und die Integrität der Informationen. Einer der grundlegenden Vorteile ist die Pseudonymisierung der Identität der beteiligten Akteure. In einer Blockchain sind die Identitäten durch kryptografische Schlüssel repräsentiert, was bedeutet, dass persönlicher oder unternehmensbezogener Daten nicht direkt sichtbar sind. Statt echter Namen oder Unternehmensinformationen erscheinen lediglich kryptografische Hashes oder Adressen.

Transparenz und Risiken

Trotz der Pseudonymisierung birgt die Blockchain-Technologie auch gewisse Risiken in Bezug auf die Privatsphäre. Da alle Transaktionen in der Blockchain offen und unveränderlich sind, können sämtliche Tokens, die einer Identität gehören, nachvollzogen werden, sobald die Kennung dieser Identität bekannt ist. Dies könnte potenziell zu Datenschutzproblemen führen, insbesondere wenn sensible Informationen durch Rückschlüsse aufgedeckt werden können.

Mitigation durch GrünstromNachweise

Die Einführung von Optionen in Form von GrünstromNachweisen bietet eine effektive Methode zur Minderung dieser Risiken. In der Praxis ist lediglich dem Auditor die Kennung der wirtschaftlich agierenden Entität vollständig bekannt. Die wirtschaftlich agierende Entität kann mehrere Kennungen nutzen, wobei für jeden Herkunftsnachweis eine Option erstellt wird, die einer neuen Kennung zugeordnet ist. Dies bedeutet, dass die eigentliche Identität des Besitzers nicht ohne weiteres nachvollzogen werden kann.

> Eine wirtschaftlich agierende Entität (z. B. ein Unternehmen) erstellt einen GrünstromNachweis für eine bestimmte Energiemenge. Dieser Nachweis wird einer neuen Kennung zugeordnet und eine Option darauf wird genutzt, um eine Verbindung zu einem Dritten herzustellen. Der Dritte kann den Herkunftsnachweis prüfen und validieren, ohne die ursprüngliche Identität der wirtschaftlich agierenden Entität offenlegen zu müssen.

Zero Knowledge Proofs

Dieses System ermöglicht die Implementierung von Zero Knowledge Proofs (ZKP), einem Verfahren, bei dem eine Partei (der Prüfer) die Richtigkeit einer Aussage verifizieren kann, ohne zusätzliche Informationen über den Inhalt der Aussage zu erhalten.

Anwendung in diesem Konzept

- Eine wirtschaftlich agierende Entität erstellt eine Option auf einen GrünstromNachweis, der einer neuen anonymen Kennung zugeordnet ist.
- Ein Dritter prüft, ob der Herkunftsnachweis existiert und valide ist, sowie ob die neue Kennung tatsächlich Anteile daran hält.
- Der Prüfer kann so die Gültigkeit der Transaktion verifizieren, ohne Zugang zu anderen vertraulichen Informationen zu erhalten.

Datenintegrität durch Blockchain-Validatoren

Die Integrität der Daten wird durch die Validatoren der zugrunde liegenden Blockchain-Technologie sichergestellt. Diese Validatoren führen kontinuierlich Überprüfungen durch, um die Echtheit und Unveränderlichkeit der Daten zu gewährleisten. Folgende Mechanismen tragen zur Datenintegrität bei:

- **Kryptografische Sicherung:** Jede Transaktion ist kryptografisch gesichert, um Manipulation oder unbefugten Zugriff zu verhindern.
- **Dezentralisierung:** Durch das dezentrale Netzwerk der Validatoren wird die Unversehrtheit der Daten gestärkt, da ein Konsensmechanismus Manipulationen nahezu unmöglich macht.
- **Transparenz:** Alle Transaktionen und Änderungen sind auf der Blockchain öffentlich einsehbar und nachprüfbar, ohne persönliche Daten offenzulegen.

Praktische Umsetzung

In der Praxis bleibt die Kennung der wirtschaftlich agierenden Entität dem Auditor bekannt, der somit als Vertrauensinstanz agiert. Die Verwendung mehrerer Kennungen und die Zuweisung von Optionen auf Herkunftsnachweise zu neuen Kennungen bietet dabei eine starke Abstraktionsebene zur Sicherstellung der Privatsphäre.

- **Mehrfachkennungen:** Eine wirtschaftlich agierende Entität kann mehrere Identitäten nutzen, um ihre Transaktionen zu verschleiern und zugleich den Datenschutz zu gewährleisten.

- **Zuweisung von Optionen:** GrünstromNachweise werden als Optionen zu neuen Kennungen zugewiesen, was die Rückverfolgbarkeit erschwert und den Datenschutz erhöht.
- **Technologie des Zero Knowledge Proofs:** Diese Technologie wird genutzt, um die Validität von Transaktionen zu überprüfen, ohne vertrauliche Informationen preiszugeben.

Zusammenfassung

Die Kombination aus Pseudonymisierung, GrünstromNachweisen und der Nutzung von Zero Knowledge Proofs bietet eine robuste Lösung zur Gewährleistung des Datenschutzes innerhalb der digitalen Nachweisführung und Tokenökonomie. Diese Maßnahmen sorgen dafür, dass sensible Daten geschützt bleiben, während gleichzeitig Transparenz und Nachvollziehbarkeit durch die Technologie der Blockchain und deren Validatoren gewährleistet sind. Unternehmen können somit ihre Scope 2-Berichterstattung sicher und datenschutzkonform optimieren.

Revision #1
Created 17 June 2024 00:48:21 by Thorsten Zoerner
Updated 12 July 2024 23:00:10 by Thorsten Zoerner