Heiko Pereira Wolf
Master of Laws
Master of Public Management

heiko.pereirawolf@hspv.nrw.de

Köln, 1. November 2024

Whitepaper V0.1 DE

Heros-Protokoll

Verwaltung von Einsatztagebüchern im Zivil- und Katastrophenschutz auf der Basis von Blockchain-Technologie

1. Einleitung

Der Zivil- und Katastrophenschutz stellt hohe Anforderungen an die Dokumentation von Einsätzen, um Transparenz, Nachvollziehbarkeit und Datensicherheit zu gewährleisten. Einsatztagebücher sind hierbei von zentraler Bedeutung, da sie die Abläufe, Entscheidungen und Entwicklungen während eines Einsatzes festhalten. Das **Heros-Protokoll** nutzt die Blockchain-Technologie, um Einsatztagebücher sicher und dezentral zu führen, zu validieren und zu archivieren. Diese Blockchain-basierte Plattform bietet eine flexible und robuste Dokumentationsstruktur, die den Anforderungen von Einsatzkräften und Führungsebenen gerecht wird.

2. Ziel des Heros-Protokolls

Das Ziel des Heros-Protokolls ist es, eine **Permissioned Blockchain** zu schaffen, auf der Einsatztagebücher im Zivil- und Katastrophenschutz effizient geführt, fortgeführt und sicher abgelegt werden können. Einsatzkräfte können Einträge in dezentralen Einsatztagebüchern erstellen, die durch strikte Verschlüsselungs- und Zugriffskontrollen gesichert und durch verschiedene Knotenstrukturen validiert und archiviert werden.

3. Funktionsweise und Struktur des Heros-Protokolls

3.1 Einsatztagebuch und Zugriffssteuerung

- **Einsatztagebücher als Wallets**: Jedes Einsatztagebuch wird wie ein digitales **Wallet** behandelt. Einsatzkräfte können beliebig viele Einsatztagebücher parallel beginnen, und nur der jeweilige Ersteller kann Einträge hinzufügen.

- **Schlüsselverwaltung**: Ein **Transferkey** wird beim Erstellen eines Einsatztagebuches generiert und erlaubt es, das Einsatztagebuch an eine andere Person zu übergeben, die damit das Hinzufügen neuer Einträge und das Erstellen weiterer View- und Transferkeys übernimmt. Das Recht des ursprünglichen Erstellers zum Hinzufügen von Einträgen erlischt mit der Übergabe. **Viewkey** ist ein schreibgeschützter Schlüssel, der an Führungskräfte und übergeordnete Führungsstellen herausgegeben wird, damit sie Einträge im Einsatztagebuch einsehen können. Der Inhaber des Transferkeys kann mehrere Viewkeys für sein Einsatztagebuch erstellen, die an unterschiedliche Personen ausgegeben werden können. Zusätzlich haben die Zentral-Knoten die Berechtigung, Viewkeys für alle Einsatztagebücher zu generieren und bestehende Viewkeys zentral zurückzuziehen, um den Zugriff gegebenenfalls zu entziehen.

- **Verknüpfung nach Schlüsselverlust**: Sollte der Transferkey verloren gehen, kann der Benutzer ein neues Einsatztagebuch eröffnen und im ersten Eintrag auf das ursprüngliche, nicht mehr weitergeführte Einsatztagebuch verweisen, um eine lückenlose Nachvollziehbarkeit zu gewährleisten.

- **Verschränkte Einträge**: Jeder Eintrag (vergleichbar mit einer Transaktion) in einem Einsatztagebuch ist kryptographisch mit dem vorherigen Eintrag verknüpft, um eine vollständige Chronologie und Integrität der Dokumentation sicherzustellen. Alle Einträge sind unveränderlich, sodass die Datenintegrität gewahrt bleibt. Falls bestimmte Einträge überholt sind, können diese als „obsolet“ markiert werden, indem auf sie in neuen Einträgen referenziert wird, ohne dass sie gelöscht werden.

4. Aufbau der Blockchain und Knotenstruktur

Das Heros-Protokoll basiert auf einer mehrschichtigen Knotenarchitektur, die aus **Archiv-Knoten**, **Portal-Knoten** und **Zentral-Knoten** besteht. Jeder Knotentyp übernimmt eine spezifische Rolle im Netzwerk und trägt zur Sicherheit, Effizienz und Robustheit des Systems bei.

- **Archiv-Knoten**: Diese Knoten sind für die dauerhafte Archivierung aller Einsatztagebücher zuständig und speichern die Blockchain in ihrer Gesamtheit. Sie gewährleisten, dass alle Einträge langfristig und redundant gespeichert sind, selbst bei Ausfällen oder dem Ausstieg einzelner Knoten.

- **Portal-Knoten**: Die Portal-Knoten steuern den Zugang zur Blockchain. Sie arbeiten nach dem **Practical Byzantine Fault Tolerance (PBFT)**-Mechanismus, um sicherzustellen, dass auch bei einem gewissen Anteil an nicht erreichbaren oder kompromittierten Knoten der Zugang zur Blockchain gesichert bleibt. PBFT stellt sicher, dass Konsens unter den Knoten erreicht wird, selbst wenn einige Knoten fehlerhaft oder kompromittiert sind. Ein neuer Eintrag wird dabei an hinreichend viele Portal-Knoten gleichzeitig adressiert, sodass selbst bei potenziell fehlerhaften oder kompromittierten Knoten genügend korrekte Portal-Knoten erreichbar sind, um Einträge effizient zu verteilen.

- **Zentral-Knoten**: Die Zentral-Knoten übernehmen die abschließende Validierung der Einträge in der Blockchain. Diese Knoten arbeiten nach dem **Proof of Authority (PoA)**-Mechanismus, bei dem nur autorisierte, vertrauenswürdige Knoten das Recht haben, neue Einträge zu validieren. Durch PoA bleibt der Validierungsprozess effizient, ohne die Sicherheit zu beeinträchtigen.

5. Sicherheit und Vertrauensmechanismen

Das Heros-Protokoll setzt verschiedene Sicherheits- und Vertrauensmechanismen ein, um den Konsens und die Verfügbarkeit der Blockchain auch unter ungünstigen Bedingungen zu gewährleisten:

- **Ausfallsicherheit und Fehlertoleranz**: PBFT und PoA gewährleisten die Integrität des Netzwerks, selbst wenn eine unbekannte Anzahl von Knoten ausfällt oder kompromittiert ist.

- **Verifizierbare Zufallsfunktion (VRF)**: Für die Auswahl und Rotierung von Portal- und Zentral-Knoten wird eine **Verifiable Random Function (VRF)** genutzt. Dies stellt sicher, dass die Auswahl kryptographisch abgesichert und manipulationssicher ist, wodurch gezielte Angriffe auf bestimmte Knoten erschwert werden.

- **Periodische Validierung und Datenreplikation**: Die Archiv-Knoten speichern die Daten redundant und werden regelmäßig durch Portal- und Zentral-Knoten auf Datenintegrität geprüft. So wird sichergestellt, dass die Blockchain-Daten auch bei teilweiser Korruption der Knoten erhalten bleiben.

6. Erweiterte Aspekte und Optimierungen

Um den Betrieb des Heros-Protokolls weiter zu verbessern und Herausforderungen zu bewältigen, werden folgende zusätzliche Punkte implementiert:

6.1 Netzwerkstabilität bei großflächigen Störungen

Sollten Knoten durch großflächige Stromausfälle oder Netzwerkausfälle isoliert werden, werden die folgenden Maßnahmen getroffen:

- **Statusüberwachung und Synchronisation**: Automatisiertes Monitoring prüft den Netzwerkstatus regelmäßig. Knoten synchronisieren ihren Stand nach Wiederherstellung der Verbindung, und ein Rollback-Mechanismus verhindert inkorrekte oder veraltete Einträge.
- **Lokale Zwischenspeicherung**: Archiv-Knoten speichern in einer redundanten Zwischenspeicherung, die nach Wiederverbindung mit dem Hauptnetzwerk abgestimmt wird, um Dateninkonsistenzen zu vermeiden.

6.2 Übergabe der Daten zwischen Portal- und Zentral-Knoten

Die Übergabe neuer Einträge erfolgt durch ein pseudo-zufälliges Verteilungsprotokoll:

- **Pseudo-Zufallsprotokoll zur Lastverteilung**: Einträge werden nach einem nachvollziehbaren Zufallsprotokoll an eine Gruppe von Portal-Knoten übergeben, wodurch ein automatisches Load-Balancing erreicht wird.
- **Batch- und Echtzeit-Protokolle**: Die Portal-Knoten übermitteln Einträge entweder in Batches oder priorisiert für kritische Einträge zur Validierung an die Zentral-Knoten. Rückbestätigungen an die Portal-Knoten sichern den validierten Stand ab.

6.3 Einsatztagebücher und DSGVO

Da Einsatztagebücher nach Artikel 2 Absatz 2 Buchstabe d DSGVO nicht dem Anwendungsbereich der DSGVO unterfallen, können alle Daten direkt und sicher auf der Blockchain verbleiben. Eine zusätzliche Off-Chain-Speicherung entfällt, was die Handhabung vereinfacht.

6.4 Weitergabe von Einsatztagebüchern

Eine Weitergabe der Einsatztagebücher an externe Instanzen ist nicht vorgesehen. Nur in Sonderfällen können Viewkeys z.B. der Staatsanwaltschaft oder Aufsichtsbehörden übermittelt werden.

6.5 Schulungs- und Testumgebungen

Zur Vorbereitung auf den Umgang mit dem Protokoll existieren drei separate Systeme:

- **Livesystem**: Für den Einsatz in echten Situationen.
- **Testsystem**: Für Simulationen und Prüfung von Updates.
- **Schulungssystem**: Für praxisnahe Schulungen. Das Protokoll wird als Open Source-Projekt veröffentlicht, um die Weiterentwicklung und Sicherheit zu fördern.

6.6 Skalierung und Lastverteilung

Die Skalierbarkeit wird durch folgende Maßnahmen sichergestellt:

- **Pseudo-Zufallsbasiertes Verteilungsprotokoll**: Anstelle eines klassischen Load Balancers wird ein pseudo-zufälliges Verteilungsprotokoll eingesetzt, um neue Einträge gleichmäßig auf die Portal-Knoten zu verteilen.
- **Geografisch verteilte Archiv-Knoten**: Eine Cluster-Organisation der Archiv-Knoten gewährleistet Redundanz und erleichtert den Zugang bei Netzwerkproblemen.

6.7 Langfristige Wartung und Verwaltung der Archiv-Knoten

Zur Gewährleistung der langfristigen Datenverfügbarkeit:

- **Planmäßiger Austausch und Wartung**: Ein Wartungsplan sichert die Verfügbarkeit durch regelmäßige Hardware- und Software-Updates.
- **Redundante Datenreplikation**: Backup-Systeme und georedundante Datenverteilung sichern die Blockchain-Daten auch bei regionalen Ausfällen.

6.8 Richtlinien zur Verantwortlichkeit und Protokollierung von Aktivitäten

Ein Audit-Trail sorgt für Transparenz und Sicherheit:

- **Zugriffskontrolle und Rechtevergabe**: Zugriffsrechte werden strikt geregelt und dokumentiert.
- **Regelmäßige Audits**: Wöchentliche und monatliche Audits stellen sicher, dass alle Aktivitäten den Vorgaben entsprechen.
- **Automatische Benachrichtigungen**: Bei verdächtigen Aktivitäten sendet das System Warnungen an verantwortliche Führungskräfte.

7. Fazit

Das **Heros-Protokoll** soll eine sichere, robuste und skalierbare Plattform zur Verwaltung von Einsatztagebüchern im Zivil- und Katastrophenschutz bieten. Die mehrschichtige Knotenstruktur, klare Zugriffskontrollen und fortschrittliche Konsensmechanismen gewährleisten eine zuverlässige Dokumentation, die Transparenz, Datenschutz und Nachvollziehbarkeit garantiert. Die zusätzlichen Mechanismen für Netzwerkresilienz, Skalierung und Wartung machen das Protokoll zu einer zukunftsfähigen Lösung im Katastrophenschutz.

Hinweise zur Unabhängigkeit und Verantwortlichkeit

Der Unterzeichner ist hauptamtlich als Beamter bei einer Bundesoberbehörde tätig und nebenamtlich Lehrbeauftragter für Allgemeines Verwaltungsrecht und Juristische Methodik an der Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen (HSPV NRW) in der Abteilung Köln.

Die Entwicklung des vorliegenden Dokumentes erfolgte unabhängig und wird weder von der genannten Hochschule noch von anderen Institutionen oder Dritten finanziert oder inhaltlich beeinflusst.