Blockchain Initiative Austria

Systembeschreibung und Rahmenbedingungen

Inhalt

1. Einleitung

Der Verein “Blockchain Initiative Austria” bezweckt:

- Die Unterstützung des Aufbaus einer sicheren, vertrauenswürdigen und dauerhaften Blockchain-Infrastruktur für die privatwirtschaftliche Nutzung.
- Die Einrichtung einer (Diskussions-) Plattform zur Organisation und Moderation der Weiterentwicklung von dazu notwendigen Themen (technisch, rechtlich, organisatorisch …).
- Die Unterstützung der Definition und Umsetzung von Anwendungsfällen im Zusammenhang mit Blockchain-Technologien.

Dieses Dokument beschreibt die Rahmenbedingungen (Regeln) für den Aufbau und Betrieb der Blockchain-Infrastruktur durch die Vereinsmitglieder.

Die vorliegende Version beschreibt die grundlegenden Bedingungen. Detaillierungen werden im Laufe der Zeit definiert werden, u.a. läuft gerade ein Projekt (AUSTRIAPRO gemeinsam mit dem Austrian Blockchain Center), wo ibs. Themen wie Governance, Recht, Datenschutz etc. behandelt werden. Die Ergebnisse werden dann jeweils vorgestellt und nach Abstimmung der Vereinsmitglieder im Rulebook entsprechend ergänzt.

2. Begriffsbestimmungen

„Konsortium Blockchain“: Eine Variante des Aufbaus eines Blockchain-Netzes, wo die Betreiber der Blockchain-Knoten (Nodes) einem „Konsortium“ (hier Verein) angehören. Es wird technisch

sichergestellt, dass nur Teilnehmer Daten in die Blockchain schreiben können. Knoten mit Read-Only Zugriff sind möglich (z.B. betrieben durch „unabhängige Dritte“). Ein weiterer Vorteil einer derart aufgebauten Blockchain liegt darin, dass dabei im Gegensatz zu öffentlichen Blockchains kein unnötig hoher Energiebedarf (durch „proof of work“) gegeben ist.

„Dokumenten-Notarisierung“: Der erste Anwendungsfall, der vom Verein aufgebaut wird. Mit Hilfe dieser Anwendung kann die Integrität von elektronischen Dokumenten (d.h. allen Arten von Dateien) sichergestellt werden. Durch die Hinterlegung eines Hashwertes (digitalen Fingerabdrucks) von Daten in der Blockchain kann später bewiesen werden, dass die Daten zum betreffenden Zeitpunkt in einer bestimmten Form vorgelegen sind und seither nicht verändert wurden. Ein System, welches diesen Anwendungsfall implementiert wird „DocNoS“ (Dokumenten-Notarisierungs-System) genannt.

„DatNoS“: Daten-Notarisierungs-System: Eine Erweiterung von DocNoS, wo auch Daten selbst im Rahmen einer Blockchain-Anwendung abgelegt werden (kommende Erweiterungen). Die im gegenständlichen Rahmen eingesetzte Blockchain-Instanz trägt bereits den Namen „datnos“.

„Austrian Public Sector Blockchain“: Eine Konsortialblockchain, an der Institutionen des öffentlichen Bereiches in Österreich teilnehmen. Die erste Anwendung der „APSB“ betrifft auch die Notarisierung, wird jedoch „Daten-Zertifizierung“[1] genannt. Die Blockchain des Vereines ist quasi als B2B-Pendant der APSB zu sehen, da sie im Gegensatz zur APSB (auch) der gesamten Privatwirtschaft (Unternehmen, Institutionen usw.) zur Verfügung steht.

3. Technik

3.1. Blockchain Umgebung

Als Blockchain-Umgebung wird das System „MultiChain“ verwendet, siehe https://www.multichain.com/

Es wird die OpenSource Version „Community Edition“ eingesetzt – Lizenz: GPLv3 - https://github.com/MultiChain/multichain

3.2. Systemanforderungen - Empfehlungen

Die Leistungsanforderungen hängen u.a. vom Einsatzzweck des Nodes ab, pro Instanz sind etwa folgende Ausstattungsmerkmale empfohlen:

- „Minimaler“ Node: nur Synchronisieren der Blockchain, kein POA-Mining, kein API, d.h. keine Transaktionen erstellen: 1 CPU, 2GB RAM
- Maximale Funktionalität: 2 CPU, 8GB RAM

- Disk (empfohlen SSD) >= 50 GB
- Betriebssystem
  - Empfohlen: Ubuntu latest LTS (derzeit 20.04 LTS)
  - Alternativen siehe https://www.multichain.com/download-community/

3.3. Inbetriebnahme

Beim ersten Start der MultiChain Umgebung wird automatisch ein Schlüsselpaar (public und private key) und eine Adresse (aus dem public Key abgeleitet) generiert. Nach Übermittlung der Adresse an

[1] https://www.wko.at/service/innovation-technologie-digitalisierung/blockchain.html

den Verein[2] unter gleichzeitigem Nachweis der Identität wird die Adresse freigeschaltet, erst danach kann der Blockchain-Node in Normalbetrieb gehen (d.h. Lese- und Schreibtransaktionen durchführen).

3.4. Spezifikationen

Die für die Anwendung „DocNoS“ zu verwendende Datenstruktur ist in folgendem Dokument spezifiziert – siehe Download-Bereich auf der Vereins-Homepage:

- DocNoS_Datenstruktur_v11_20201105.pdf

4. Organisation

Unterschieden werden

- Knotenbetreiber: Betreiber von einem (oder mehreren) Blockchain-Knoten im Rahmen der „datnos“[3]-Blockchain.
- Applikationsbetreiber: Betreiber von Anwendungen, die auf Blockchain-Knoten zugreifen. Die Anwendungen stellen Services für die User (Endkunden) bereit.

Ein Applikationsbetreiber wird typischerweise seinen eigenen Knoten betreiben. Das ist aber nicht zwingend erforderlich. D.h. es kann auch API-Anbieter oder BaaS (Blockchain as a Service) geben.

5. Kommerzielles

5.1. Blockchain-Infrastruktur

Hier gelten folgende Regeln:

- Jeder Nodebetreiber trägt die Kosten für seinen eigenen Node.
- Es gibt keine Verrechnung zwischen den Node-Betreibern (Transaktionsgebühren o.ä.).
- Dies gilt nach dem „Fair-Use“ Prinzip. Sollte ein Node einen extrem hohen Anteil aller Transaktionen im Gesamtsystem durchführen, muss der Betreiber entsprechende Maßnahmen treffen (z.B. einen weiteren Node bereitstellen etc.).
- Ein Nodebetreiber kann (und wird) ggf. Leistungen gegenüber seinen Anwendungsbetreibern verrechnen.

5.2. Anwendungen

- Ein Anwendungsbetreiber kann (und wird) Leistungen gegenüber seinen UserInnen verrechnen.

6. Recht

Prinzipiell gilt, dass keine kritischen (rechtlich verbotenen) Daten in die gemeinsame Blockchain gespeichert werden dürfen. Das betrifft ibs. auch personenbezogene Daten im Rahmen der DSGVO.

Im aktuell verfügbaren Anwendungsfall DocNoS werden jedenfalls nur Hashwerte und unkritische Meta-Informationen (Zeitstempel, IDs etc.) verarbeitet. Vor Definition weiterer Anwendungen müssen

[2] Kontaktdaten siehe Ende des Dokumentes
[3] Die „datnos“-Blockchain wird auch die Basis für weitere Applikationen sein

jedenfalls die rechtlichen Rahmenbedingungen ganz klar definiert werden, was derzeit im o.a. Projekt (AUSTRIAPRO mit Austrian Blockchain Center) geschieht.

Bei Verstößen gegen o.a. Regeln können die lt. 3.3 vergebenen Lese-/Schreibrechte entzogen werden und ggf. weitere Maßnahmen gesetzt werden.

7. Kontakt

Verein “Blockchain Initiative Austria”
Anton-Krieger-Gasse 83
A-1230 Wien
Mail: hello@bc-init.at
Web: https://bc-init.at