

Austrian Public Service Blockchain Leitfaden und Vereinbarung

Doku-Klasse:
ergänzend

Kurzbezeichnung:
APSB-LV-1.0

Kurzbeschreibung: Die Blockchain-Technologie kann die Unverfälschtheit von Daten aus technischer Sicht beweisen. Sie ist daher ein geeignetes Mittel, das Vertrauen in E-Government zu stärken.

Damit einzelne Projekte im öffentlichen Bereich die Technologie anwenden können, sowie Wissen zur Nutzung der Technologie aufbauen können, steht eine Blockchain-Infrastruktur für Österreich „Austrian Public Service Blockchain (APSB)“ für die Speicherung von nicht personenbezogenen Hashwerten zur Verfügung.

Im Leitfaden werden Standards und Empfehlungen zur Nutzung der APSB erklärt, die bei allen österreichischen Verwaltungen für den Betrieb von Blockchain-Knoten und darauf basierenden Anwendungen zur Anwendung kommen können.

In der Vereinbarung werden Gegenstand und Zweck der APSB, Architektur, Rechte und Pflichten, sowie Haftung der APSB-Teilnehmer:innen erläutert.

Verfasst von: Brigitte Lutz

Projektteam/Arbeitsgruppe: Austrian Public Service Blockchain

Version / Datum: V1.0 / 16.02.2022

Doku-Stadium: Ergebnis der AG

Gültig seit: 05.12.2022

Nächste Überprüfung am: 05.12.2024

Inhaltsverzeichnis

Management Summary	3
Einleitung	3
1 Leitfaden	4
1.1 Grundsätze der Infrastruktur	4
1.2 Technische Gründung	6
2 Vereinbarung	7
2.1 § 1 Gegenstand und Zweck des Austrian Public Service Blockchainsystems	7
2.2 § 2 APSB Architektur	7
2.3 § 3 Begriffsbestimmungen	8
2.4 § 4 Beitritt zur APSB	10
2.5 § 5 Rechte und Pflichten von Anwendungsverantwortlichen.....	10
2.6 § 6 Rechte und Pflichten des Knotenverantwortlichen	10
2.7 § 7 Technische und organisatorische Vorkehrungen	10
2.8 § 8 Haftungsregelung	11
2.9 § 9 Entzug der Teilnahme	11
2.10 § 10 Änderungen der Vereinbarung über die APSB	11
2.11 § 11 Schlussbestimmungen	11
3 Anhang	12
Abbildungsverzeichnis	13
Tabellenverzeichnis	13
Beschreibung der Abkürzung	13
Änderungsprotokoll	13

Management Summary

Die Blockchain-Technologie kann die Unverfälschtheit von Daten aus technischer Sicht beweisen. Sie ist daher ein geeignetes Mittel, das Vertrauen in E-Government zu stärken.

Die Universität Lille hat im November 2021 das [Weissbuch „Blockchain-Technologie für den öffentlichen Sektor“](#) herausgegeben, in dem Informationen über Blockchain-Technologien im Allgemeinen, sowie über sieben Anwendungsfälle enthalten sind.

Damit einzelne Projekte im öffentlichen Bereich die Technologie anwenden können, sowie Wissen zur Nutzung der Technologie aufbauen können, steht eine Blockchain-Infrastruktur für Österreich „Austrian Public Service Blockchain (APSB)“ für die Speicherung von nicht personenbezogenen Hashwerten zur Verfügung. Die dabei verwendeten Konsensalgorithmen stellen sicher, dass kein energieverschwendendes Mining betrieben wird und die Infrastruktur auch umwelt- und ressourcenschonend gestaltet ist.

Dazu wurde dieses Dokument, bestehend aus Leitfaden und Vereinbarung mit folgenden Beilagen ausgearbeitet:

Anhang 1: Vorlage für Beitrittserklärung zur APSB

Anhang 2: Technische Spezifikation (Implementierungs-Leitfaden)

Anhang 3: Präsentationsunterlagen zum APSB für das Management

Um ökonomisch zu handeln, kann ein Konsortium gegründet werden, das Weiterentwicklungen gemeinsam in Auftrag gibt und für das separate Vereinbarungen zu treffen sind, die sich an bestehenden Vereinbarungen der BLSG zur gemeinsamen Weiterentwicklung von IT-Systemen orientieren können. Der Beitritt erfolgt gesondert und ist freiwillig.

Einleitung

Im Kapitel 1 - Leitfaden werden Standards und Empfehlungen zur Nutzung der APSB erklärt, die bei allen österreichischen Verwaltungen für den Betrieb von Blockchain-Knoten und darauf basierenden Anwendungen zur Anwendung kommen können.

Im Kapitel 2 - Vereinbarung werden Gegenstand und Zweck der APSB, Architektur, Rechte und Pflichten, sowie Haftung der APSB-Teilnehmer:innen (Knotenverantwortlicher und Anwendungsverantwortlicher) erläutert.

Die Infrastruktur ist bereits im Betrieb.

Um die Blockchain in österreichischen Verwaltungen nutzen zu können, ist ein gemeinsamer Ansatz essentiell.

Die Entwicklung der European Blockchain Services Infrastructure ([EBSI](#)) wird von der Projektgruppe beobachtet und

- eine mögliche Koppelung der APSB zur EBSI entwerfen
- und auch in den Betrieb eines Nodes und in die Umsetzung von Usecases einsteigen.

1 Leitfaden

1.1 Grundsätze der Infrastruktur

Um auch die Nutzung für Unternehmen zu ermöglichen, hat der Verein „Blockchain Initiative Austria“ <https://bc-init.at/>, dessen Policygrundlagen vom Austrian Blockchain Center erarbeitet wurden, eine entsprechende sehr ähnliche weitere Infrastruktur geschaffen und in Betrieb gesetzt.

Beide Infrastrukturen haben folgende Grundsätze:

- Die verwendeten Konsensalgorithmen stellen sicher, dass kein energieverschwendendes Mining betrieben wird und die Infrastruktur auch umwelt- und ressourcenschonend gestaltet ist.
- Made in Austria, aber unter Beobachtung der EU Aktivitäten
- Anwendung von Open Source Software (Multichain)
- Personenbezogene Daten werden offchain gespeichert und sind nicht Gegenstand dieser Infrastrukturen.

Folgende Usecases im Bereich Notarisierung können damit umgesetzt werden:

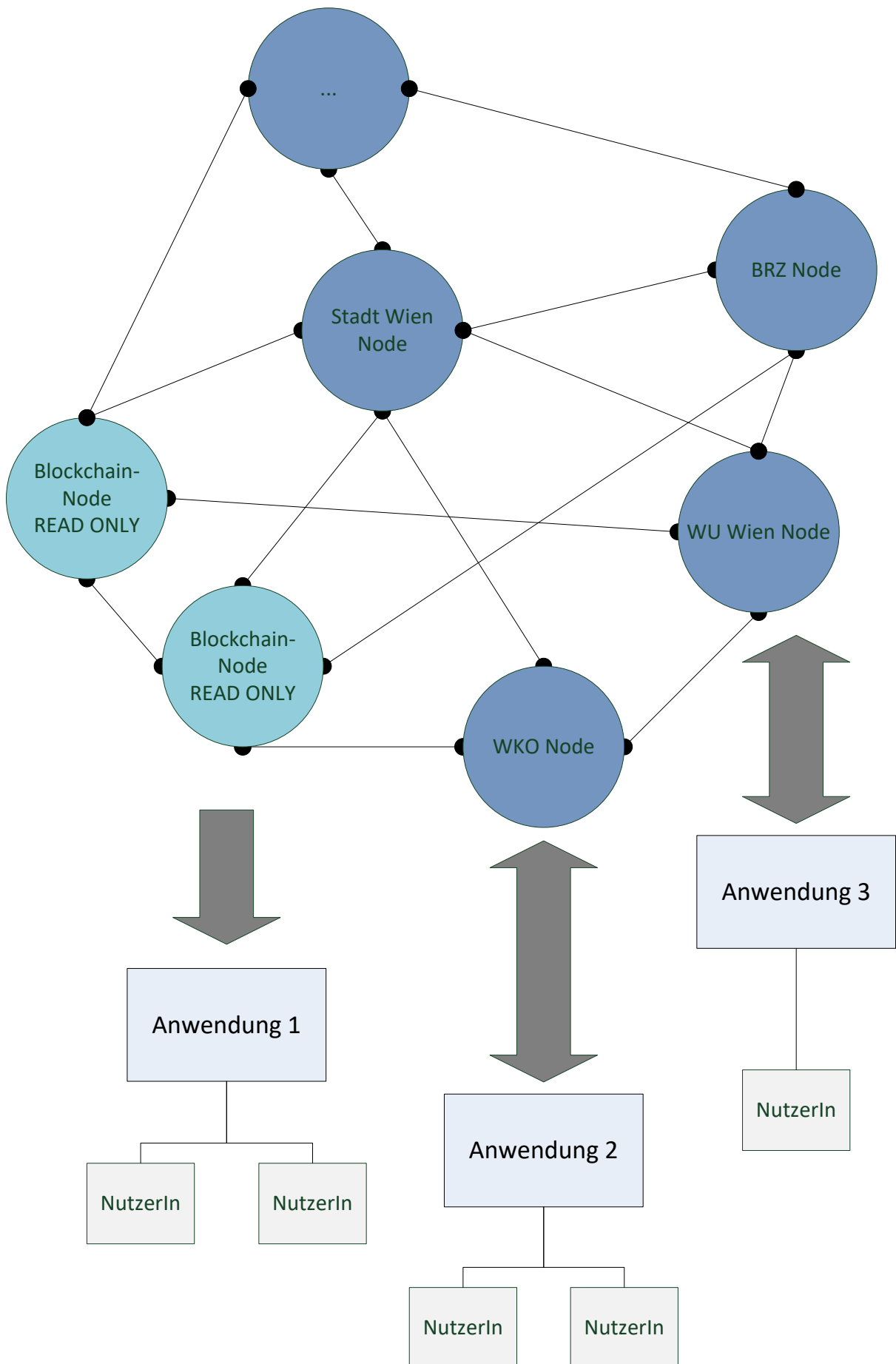
- Texte sollten (mindestens) Absatzweise übernommen werden (inkl. Absatzmarke).
- Dokumente, Daten, Pläne, Medien in jedem beliebigen digitalen Format, Zeugnisse
- Transparente Dokumentation der Überprüfung von Infrastrukturobjekten wie zB Brücken, ...
- Nachvollziehbarkeit von Datenströmen aus Sensoren (IoT,..)
- Nachvollziehbarkeit von Prozessen
- Urheberschaft (Texte, Musik, Fotos, Bilder, Videos ...)
- Akademische Integrität (zB Daten von empirischen Untersuchungen)

Die Blockchaintechnologie eignet sich hervorragend dafür, Daten langfristig und vertrauenswürdig abzuspeichern. Voraussetzung dafür ist, dass es vertrauenswürdige Partner gibt, die an dem System teilnehmen und dieses am Leben erhalten.

Ein wichtiges technisches Leitprinzip ist dabei, dass alle Daten die von einem Partner eingegeben werden, werden mit allen Knoten synchronisiert und von diesen dauerhaft gespeichert. Derzeit wird ein „Stream“ verwendet, um die Hashwerte von „notarisierten“ Files zu speichern, weitere Streams für andere Anwendungsfälle können jederzeit angelegt werden.

Wie ersichtlich, sind verschiedenste Kooperationspartner Teilnehmer:innen in diesem System. Um am System teilzunehmen, sollte ein eigener Knoten in der Austrian Public Service Blockchain betrieben werden. Das System soll umwelt- und ressourcenschonend und im Interesse aller Kooperationspartner weiterentwickelt werden.

Abbildung 1 - System Austrian Public Service Blockchain (APSB)



1.2 Technische Gründung

Folgende Organisationen haben die technische Gründung vollzogen, sodass in der Vereinbarung kein eigener Abschnitt über die Vereinbarung bzw. Gründung der APSB erforderlich ist:

- Bundesrechenzentrum (BRZ)
- Österreichische Kontrollbank AG (OeKB)
- Stadt Wien
- Wirtschaftskammer Österreich (WKO)
- Wirtschaftsuniversität Wien

2 Vereinbarung

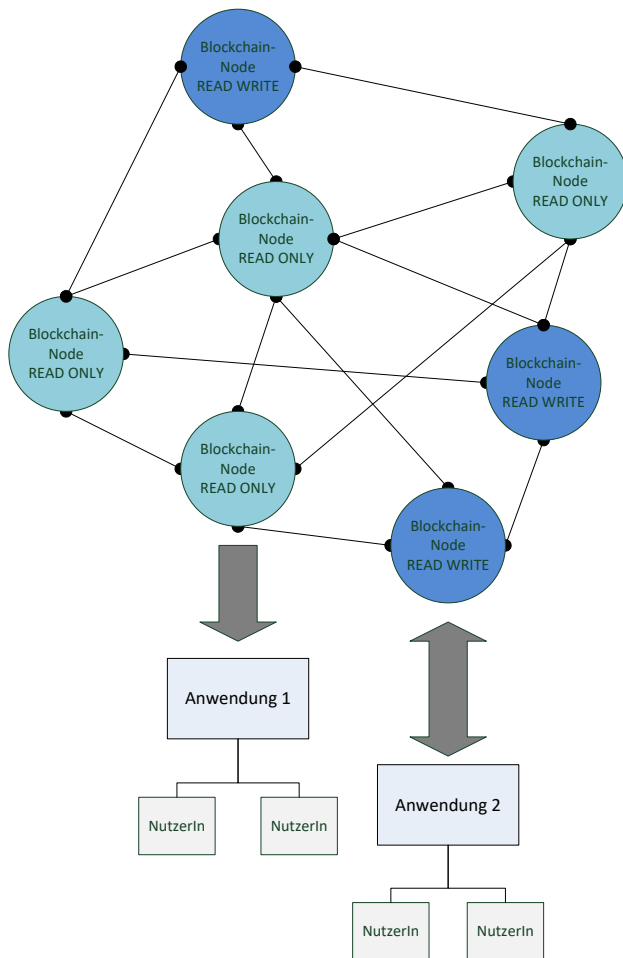
2.1 § 1 Gegenstand und Zweck des Austrian Public Service Blockchainsystems

- Ein verteiltes Datenbanksystem auf Basis einer Multichain-basierenden Blockchaintechnologie soll für den öffentlichen Bereich in Österreich die Infrastruktur für Anwendungen bieten. Dieses System wird als Austrian Public Service Blockchain (in der Folge kurz APSB) bezeichnet. Unter öffentlichem Bereich im Sinn dieser Vereinbarung fallen Bund, Länder, Städte und Gemeinden, Organisationen, die im Auftrag einer Gebietskörperschaft tätig sind (zB Oesterreichische Kontrollbank Aktiengesellschaft), Einrichtungen öffentlichen Rechts (zB Kammern) sowie Hochschulen (Universitäten und Fachhochschulen).
- Die APSB-Teilnehmer:innen erklären durch ihre jeweilige Beitrittserklärung gemäß § 4 für den von ihnen jeweils vertretenen Bereich, dass sie zum Zweck der technischen und organisatorischen Nutzung des APSB die Einhaltung der nachstehend festgelegten Rechte und Pflichten sowie Standards und die bestmögliche Umsetzung allfällig enthaltener Empfehlungen dieser Vereinbarung.
- Sie kommen weiters überein, dass der künftige Beitritt weiterer Teilnehmer:innen gemäß Abs 1 zur APSB zulässig sein soll, sofern diese ihrerseits erklären, je nach der ihnen im APSB zukommenden Rolle (vgl. §§ 5 - 6) die in dieser Vereinbarung angeführten Rechte und Pflichten sowie Standards einzuhalten und allfällig enthaltene Empfehlungen bestmöglich umzusetzen.
- Sämtliche Erklärungen nach den Absätzen 2 und 3 gelten als abgegeben, sobald sie bei dem für die IT-Koordination des Bundes zuständigen Bundesministerium als dem Depositär dieser Vereinbarung eingelangt sind. Der Depositär wird die Erklärungen unter <http://reference.e-government.gv.at> kundmachen.

2.2 § 2 APSB Architektur

- Das System besteht u.a. aus einer Art Datenbanksystem mit Bereichen („Streams“), in denen inhaltlich zusammengehörige Nutzdaten abgelegt werden.
- Im ersten einzurichtenden Bereich werden lediglich Prüfsummen von Daten (auch Dateien) (sog. Hashwerte) abgelegt, wobei Hashwerte nicht personenbezogen sein dürfen. Für die Einhaltung dieser Konvention hat jeder/jede APSB-Teilnehmer:innen zu sorgen.
- Weitere Streams können zur Speicherung anderer nicht personenbezogener Datenarten (zB Wetter, Umwelt, Erdbeobachtung) unter Einhaltung von Regelungen des § 7 Abs 2 vereinbart und eingerichtet werden.
- Die Nutzung der APSB erfolgt durch den Gebrauch von Autorisierten Blockchain-Anwendungen, die von APSB-Teilnehmer:innen betrieben werden. Die Nutzer:innen der Autorisierten Blockchain-Anwendungen selbst müssen nicht dieser Vereinbarung beitreten.

Abbildung 2 - APBS-Architektur



2.3 § 3 Begriffsbestimmungen

In der vorliegenden Vereinbarung haben die nachstehenden Begriffe folgende Bedeutung:

Tabelle 1 - Begriffsbestimmungen

<p>1. Blockchaintnoten</p>	<p>Ein IT-System auf welchem eine Blockchainumgebung (hier: Multichain) installiert ist. Blockchaintnoten arbeiten dezentral (dh unterliegen keiner zB Client-Server Struktur und sind somit alle gleichberechtigt), kommunizieren selbständig miteinander und synchronisieren dabei die Transaktionsdaten. Kryptografische Verfahren (ibs. digitale Signatur und Hashwerte) stellen dabei sicher, dass die Daten nicht manipuliert werden können, ein Konsensalgorithmus sorgt dafür, dass alle Knoten dieselben Transaktionen als valide anerkennen.</p>
----------------------------	--

2. Knotenverantwortlicher	Jener Rechtsträger oder dessen Organ, der selbst einen Blockchainknoten betreibt oder in dessen Auftrag ein Knoten betrieben wird und in dessen Verantwortung die Einräumung von Zugriffsrechten von Anwendungsverantwortlichen auf seinen Blockchainknoten fällt
3. Autorisierte Blockchain-Anwendung	Anwendung, die über einen (fremd- oder selbstbetriebenen) Blockchainknoten Daten in die APSB ablegen darf.
4. Anwendungsverantwortlicher	Jener Rechtsträger oder dessen Organ, der eine Autorisierte Blockchain-Anwendung betreibt, die auf die APSB lesend oder schreibend zugreift und in dessen Verantwortung die Einräumung von Zugriffsrechten für Nutzer:innen auf eine Autorisierte Blockchain-Anwendung fällt.
5. Depositar	<p>Der Depositar für die APSB ist das für die IT-Koordination des Bundes zuständige Bundesministerium.</p> <p>Er nimmt sämtliche Erklärungen im Rahmen der APSB entgegen und bringt sie den APSB-Teilnehmer:innen zur Kenntnis. Des Weiteren führt der Depositar eine Evidenz über die APSB-Teilnehmer:innen, die er unter https://reference.e-government.gv.at veröffentlicht. Änderungen in dieser Evidenz hat er allen APSB-Teilnehmer:innen ohne unnötigen Aufschub mitzuteilen.</p>
6. APSB-Teilnehmer:innen	Die Gesamtmenge der Knoten- und Anwendungsverantwortlichen der APSB.
7. Nutzer:innen	Nutzer:innen der Autorisierten Blockchain-Anwendungen, die außerhalb dieser Vereinbarung stehen.
8. Stream	Die APSB besteht aus Bereichen („Streams“), in denen inhaltlich zusammengehörige Nutzdaten abgelegt werden.

2.4 § 4 Beitritt zur APSB

- Der Beitrittswerber teilt mittels vollständig ausgefüllter und unterfertigter Beitrittserklärung (siehe Anhang 1) mit, der gegenständlichen Vereinbarung beitreten zu wollen und übermittelt diese an den Depositär.
- Die Beitrittserklärung wird vom Depositär sodann allen Knotenverantwortlichen zur Kenntnis gebracht.
- Der Beitritt wird wirksam, sofern nicht innerhalb von 21 Tagen entweder
 - 25 % der Knotenverantwortlichen dem Beitritt widersprechen oder
 - der Bund, vertreten durch das für die IT-Koordination des Bundes zuständige Bundesministerium oder ein Bundesland, das einen Blockchainknoten in der APSB betreibt, dem Beitritt widerspricht.

2.5 § 5 Rechte und Pflichten von Anwendungsverantwortlichen

- Der Anwendungsverantwortliche ist verantwortlich dafür, dass seine Autorisierte Blockchain-Anwendung keine personenbezogenen oder anderweitig rechtlich relevanten Daten (Strafrecht, Urheberrecht, usw.) in APSB schreibt. Er hat nach Maßgabe des jeweiligen Standes der Technik und der rechtlichen und organisatorischen Möglichkeiten die erforderlichen Datensicherheitsmaßnahmen zu organisieren und umzusetzen. Dies beinhaltet auch die Möglichkeit, einzelne Nutzer:innen von der Autorisierten Blockchain-Anwendungen auszuschließen.
- Der Anwendungsverantwortliche teilt dem Depositär rechtzeitig vorab mit, wenn er plant seine Autorisierte Blockchain-Anwendung wesentlich hinsichtlich der Zielgruppe/Nutzer:innen, den verarbeiteten Datenarten, der Frequenz, der Verfügbarkeit zu ändern oder die Ansprechpartner:innen der Teilnehmer:innen für allfällige Rückfragen wechseln. Gleiches gilt für die Inbetriebnahme von neuen Anwendungen.

2.6 § 6 Rechte und Pflichten des Knotenverantwortlichen

- Der Knotenverantwortliche stellt sicher, dass nur Autorisierte Blockchain-Anwendungen gemäß § 3 Z 4 auf seinen Blockchainknoten zugreifen.
- Er hat nach Maßgabe des jeweiligen Standes der Technik und der rechtlichen und organisatorischen Möglichkeiten die erforderlichen Datensicherheitsmaßnahmen in angemessener Zeit zu organisieren und umzusetzen.
- Mindestverfügbarkeiten der jeweiligen Blockchainknoten festzulegen ist aufgrund der dezentralen Architektur des Blockchainsystems nicht notwendig.
- Er hat dafür Sorge zu tragen, dass sich die Anwendungsverantwortlichen, die seinen Blockchainknoten verwenden, an die maßgeblichen Bestimmungen bzgl. der Verwendung in dieser Vereinbarung halten.

2.7 § 7 Technische und organisatorische Vorkehrungen

- Betrieb und Weiterentwicklung der APSB
 - Um ökonomisch zu handeln, kann ein Konsortium gegründet werden, das Weiterentwicklungen gemeinsam in Auftrag gibt. Der Beitritt erfolgt gesondert und ist freiwillig. (Siehe Anhang 3: Kooperationsvereinbarung)
- Einrichtung neuer Streams der Blockchain
 - Ein/eine APSB-Teilnehmer:in kann im Wege einer Ergänzung dieser Vereinbarung die Einrichtung eines neuen Streams in der APSB durch Mitteilung an den Depositär beantragen. Die Mitteilung hat detaillierte Informationen zur beabsichtigten Nutzung sowie Art der gespeicherten Daten zu enthalten. § 4 Abs 2 und 3 gelten sinngemäß.
- Depositär teilt Knotenbetreibern Meldungen gem. § 5 Abs 2 und 7 Abs 2 mit.

2.8 § 8 Haftungsregelung

- Die APSB-Teilnehmer:innen kommen überein, wechselseitig auf jedwede Haftung, soweit gesetzlich möglich, zu verzichten. Dieser Ausschluss umfasst daher jedenfalls Fälle leichter Fahrlässigkeit und allenfalls auch gröbere Sorgfaltsverletzungen (schlichte grobe Fahrlässigkeit).
- Die Haftung von Anwendungsverantwortlichen für Verstöße gegen die Bestimmungen gemäß § 2 Abs (2) und § 5 (1) dieser Vereinbarung sind von diesem Verzicht ausdrücklich nicht umfasst.

2.9 § 9 Entzug der Teilnahme

- Der Anwendungsverantwortliche verpflichtet sich einen/eine Nutzer:in von der Nutzung seiner/ihrer Autorisierten Blockchain-Anwendung auszuschließen, wenn
 - ihm ein diesbezügliches begründetes Verlangen seines Knotenverantwortlichen zugegangen ist, oder
 - dem Anwendungsverantwortlichen zur Kenntnis gelangt, dass der/die Nutzer:innen die Autorisierte Blockchain-Anwendung missbräuchlich verwendet.
- Der Knotenverantwortliche ist berechtigt, in begründeten Fällen, einzelne seiner Autorisierten Blockchain-Anwendungen von der weiteren Nutzung seines Blockchainknotens selbst unmittelbar auszuschließen. Der Knotenverantwortliche ist bei vereinbarungswidriger Verwendung der APSB durch seine Autorisierten Blockchain-Anwendungen verpflichtet diese von der weiteren Nutzung seines Blockchainknotens selbst unmittelbar auszuschließen.

2.10 § 10 Änderungen der Vereinbarung über die APSB

- Notwendige Änderungen dieser Vereinbarung und der Anhänge werden durch die zuständige Projektgruppe der BLSG ausgearbeitet und allen Ländern, dem Bund, dem Österreichischen Städtebund und dem Österreichischen Gemeindebund zur Abstimmung vorgelegt. Die neue verbindliche Version wird unter <https://reference.e-government.gv.at> kundgemacht. Davon werden alle APSB-Teilnehmer:innen verständigt.
- Dabei wird nach Möglichkeit versucht, entsprechende Übergangszeiträume für die Einführung neuer Funktionen vorzusehen.

2.11 § 11 Schlussbestimmungen

- Jeder/jede APSB-Teilnehmer:in kann durch entsprechende schriftliche Erklärung aus dem APSB austreten. Dieser Austritt wird 1 Monat nach Einlangen der Erklärung beim Depositar wirksam.
- Im Fall einer Änderung dieser Vereinbarung gemäß § 9 kann jeder/jede APSB-Teilnehmer:in, der mit den Änderungen nicht einverstanden ist, durch Erklärung an den Depositar aus der APSB mit sofortiger Wirkung austreten.
- Die Teilnahme an der APSB ist für die APSB-Teilnehmer:innen kostenlos.
- Jeder/jede APSB-Teilnehmer:in trägt die Kosten, die sich für ihn beim Beitritt, während der Teilnahme, oder beim Austritt aus der APSB ergeben, selbst.

3 Anhang

Anhang 1: Vorlage für Beitrittserklärung zur APSB

Anhang 2: Technische Spezifikation (Implementierungs-Leitfaden)

Anhang 3: Präsentationsunterlagen zum APSB für das Management

Abbildungsverzeichnis

Abbildung 1 - System Austrian Public Service Blockchain (APSB)	5
Abbildung 2 - APBS-Architektur	8

Tabellenverzeichnis

Tabelle 1 - Begriffsbestimmungen	8
--	---

Beschreibung der Abkürzung

Beschreibung der Abkürzungen

- APSB – Austrian Public Service Blockchain
- BRZ – Bundesrechenzentrum
- WKO – Wirtschaftskammer Österreich
- WU Wien – Wirtschaftsuniversität Wien
- EBSI – European Blockchain Services Infrastructure

Änderungsprotokoll

Version X zu Y

Datum:

Autor:in:

Änderungen