

ICS 35.030; 35.240.99

Blockchain-basierte Datenvalidierung; Text Englisch

Blockchain-based validation of data; Text in English

Validation des données basée sur la chaîne de blocs; Texte en anglais

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 14 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.

Contents

	Page
Forword.....	3
Introduction.....	4
1 Scope	5
2 Normative references	5
3 Terms and definitions.....	6
4 General characteristics of blockchain validation	8
5 Technical framework of blockchain validation.....	9
5.1 Steps of the blockchain validation process	9
5.2 Cryptographic components.....	10
5.2.1 Hash functions	10
5.2.2 Digital signatures.....	10
5.3 Output of the blockchain validation process.....	10
6 Technical framework of the verification of blockchain validation	11
6.1 Introduction.....	11
6.2 Steps of the verification of an existing blockchain validation.....	11
6.3 Elements of the verification of an existing blockchain time-stamp.....	12
6.3.1 Overview and application rules	12
6.3.2 Affirmation.....	12
6.3.3 Evaluating immutability (based on proof of work).....	12
6.3.4 Blockchain time-stamp accuracy	13
Bibliography	14

Forword

This DIN SPEC has been developed according to the PAS procedure. The development of a DIN SPEC according to the PAS procedure is carried out in workshops and does not require the involvement of all stakeholders.

This document has been developed and adopted by the initiator(s) and authors named below:

- Dr. Eyal Ron
Cryptom Technologies, Berlin
- Dr. Simone Wurster
TU Berlin, FG Innovationsökonomie, Berlin
- Craig Sailor
Cryptom Technologies UG, Berlin
- Bruce Pon
BigchainDB GmbH, Berlin
- Masha McConaghy
BigchainDB GmbH, Berlin
- Steffen Schwalm
msg systems AG, Berlin
- Detlef Olschewski
Cleopa GmbH, Hennigsdorf
- Florian Glatz
Legal Tech Center, Berlin
- Matthias Möller
Bot Labs GmbH, Berlin
- Simon Schwerin
XAIN AG, Berlin

At present, there are no standards covering this topic. DIN SPECs are not part of the body of German standards. A draft of this DIN SPEC has not been published.

Despite great efforts to ensure the accuracy, reliability and precision of technical and non-technical information, the Workshop cannot give any explicit or implicit assurance or warranty in respect of the accuracy of the document. Users of this document are hereby made aware that the Workshop cannot be held liable for any damage or loss. The application of this DIN SPEC does not release users from the responsibility for their own actions and is applied at their own risk.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. DIN shall not be held responsible for identifying any or all such patent rights.

Provision of this document free of charge as a PDF via the Beuth Webshop has been financed in advance.

Introduction

This document is part of the project BlockOne – DIN SPECS “Terminology for blockchains” and “Use Case ‘blockchain notary’”.¹⁾

We thank numerous experts for their helpful input. In particular, we thank Dr. Sebastian Schmittner for his valuable support.

1) See http://www.inno.tu-berlin.de/menue/research/projects/blockone_din_specs_terminology_for_blockchains_and_use_case_blockchain_notary/ for details.

1 Scope

This DIN SPEC specifies the technical framework and functions of blockchain validation software for blockchain validation processes. In particular, it provides requirements and evaluation criteria for blockchain proof of correctness and blockchain time-stamping functional aspects.

The evaluation criteria are given for public proof of work blockchains, as these are the main ones being used in blockchain validation software [1]. The criteria do not specify when blockchain time-stamps are considered good, but instead require the software to provide the users with sufficient information to make a judgment on their own.

Other functional aspects of blockchain validation software, in particular the identification of users and the storage of data, as well as topics involving the development of the software itself, such as quality assurance, are not covered by this document.

This DIN SPEC is aimed towards blockchain validation software users. A discussion regarding the software of public proof of work blockchain themselves is not part of this specification.

This document is applicable to blockchain-based validation in general as well as specific applications, such as:

- proof of physical and intellectual property rights (except form requirements),
- declarations of intent (except written form requirements),
- public registers,
- website and accounting document validation,
- facilitating blockchain-based validation of documents in a multinational environment and
- energy networks and SmartMeter technologies.

The certification and notarization of documents is not in scope of this document as these processes are specified by national and European law.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 10118-3, *Information technology — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 14888-3, *IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*