Zuverlässigkeit von Verteiltem Juridical Recording

The reliability of Distributed Juridical Recording

Jens Braband | Hendrik Schäbe

Das Projekt RailChain beschäftigt sich mit der Übertragbarkeit von Blockchain- und Distributed-Ledger-Technologien in den Bahnbetrieb und wird durch das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) im Programm mFund gefördert. Das Projektkonsortium besteht aus der DB Systel GmbH, der Siemens Mobility GmbH, der Siemens AG, dem Hasso-Plattner-Institut der Universität Potsdam, der Technischen Universität Braunschweig, der TÜV Rheinland InterTraffic GmbH und der Spherity GmbH. Bevor auf die Anwendung an sich eingegangen wird, soll zu Beginn kurz auf Blockchain und ihre Ausprägungen eingegangen werden, um ein Verständnis für die Möglichkeiten, aber auch Grenzen zu schaffen.

1 Grundlagen zu Blockchain

Im Prinzip ist eine Blockchain eine kontinuierlich erweiterbare Liste von Datensätzen, auch Blöcke genannt, die mittels kryptographischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptographischen Fingerabdruck (Hash) des vorhergehenden Blocks, einen Zeitstempel sowie weitere Transaktionsdaten. Dabei ist wesentlich, dass die Teilnehmer an einer Blockchain verteilt sind und sich nicht notwendigerweise vertrauen müssen. Aber zumindest zu bestimmten Zeitpunkten muss Konsens über die Korrektheit der Datensätze hergestellt werden können, und zwar von jedem Teilnehmer unabhängig. D. h. man kann eine Blockchain auch als eine verteilte Datenbank ansehen, deren Daten synchronisiert werden und die unter gewissen Randbedingungen gegen Manipulation geschützt ist. Daher spricht man oft auch von einem Distributed Ledger (im Sinne von Verteilte Buchführung), da sich die Teilnehmer über den Zustand dieses verteilten „Hauptbuches" einigen wollen.

Blockchain- bzw. Distributed-Ledger-Technologien sind in ihrer bekanntesten Ausprägung [5], deren prominenteste die Kryptowährung BitCoin darstellt, für Steuerungsanwendungen in der Eisenbahn ungeeignet, obwohl sie auch hier neuartige Anwendungen ermöglichen könnten [6]. Die bisher existierenden Lösungen können weder die notwendigen Echtzeitanforderungen erfüllen noch Konsens zu jedem Zeitpunkt garantieren. In der Ethereum-Blockchain wird z. B. höchstens ca. alle 15 Sekunden ein Block erstellt, wodurch die finale Konsensfindung mehrere Minuten dauern kann. Solange können die Einträge in der Blockchain nicht als sicher oder endgültig angesehen werden. Außerdem ist der hohe Energieverbrauch bei öffentlichen Blockchains wie Bitcoin für ein umweltfreundliches Verkehrsmittel indiskutabel. Aber auch die zugrundeliegenden Basistechnologien sind noch nicht ausgereift, geschweige denn standardisiert.

Trotzdem haben Blockchain- bzw. Distributed Ledger-Technologien und insbesondere die Verwendung von Smart Contracts (das sind Protokolle, die beliebige Verträge abbilden, überprüfen und abwickeln können) in hochgradig verteilten Infrastrukturen, wie es Eisenbahnanwendungen sind, ein hohes Potenzial. Dies gilt insbesondere vor dem Hintergrund der fortschreitenden Fragmentierung und Privatisie-

The RailChain project is involved with the transferability of Blockchain and distributed ledger technologies to rail operations. It is funded by the Federal Ministry of Transport and Digital Infrastructure (BMVI) from the mFund program. The project consortium consists of DB Systel GmbH, Siemens Mobility GmbH, Siemens AG, the Hasso Plattner Institute of the University of Potsdam, the Technical University of Braunschweig, TÜV Rheinland InterTraffic GmbH and Spherity GmbH. Before the application of Blockchain itself is discussed, Blockchain and its characteristics will be briefly discussed in order to provide an understanding of its possibilities, but also its limits.

1 Blockchain basics

In principle, a Blockchain is a continuously expandable list of data records, also called blocks, that are linked together using cryptographic methods. Each block typically contains a cryptographic fingerprint (hash) of the previous block, a time stamp and further transaction data. It is quintessential that the participants in a Blockchain are distributed and do not necessarily have to trust each other. However, it must be possible to establish a consensus about the correctness of the data records, regardless of each participant, at least at certain times. Therefore, a Blockchain can also be viewed as a distributed database, the data of which is synchronised and protected against manipulation under certain boundary conditions. Therefore, we often speak of a distributed ledger (in the sense of distributed accounting), because the participants want to agree on the status of any such distributed "general ledger".

Blockchain or distributed ledger technologies in their best-known form [5], the most prominent of which is the cryptocurrency Bitcoin, are unsuitable for railroad control applications, although they could also enable novel applications there [6]. The existing solutions can neither meet the necessary real-time requirements nor guarantee consensus at all times. In the Ethereum Blockchain, for example, a block is created every 15 seconds at the most, so it can take several minutes to reach a final consensus. The entries in the Blockchain cannot be considered safe or final until then. In addition, the high energy consumption of public Blockchains such as Bitcoin is out of the question for an environmentally friendly means of transport. However, the underlying basic technologies have also not yet been fully developed, let alone standardised.

Nevertheless, Blockchain or distributed ledger technologies and in particular the use of smart contracts (these are protocols that can map, check and process any contracts) have great potential in highly distributed infrastructures, such as railway applications. This is particularly true in connection with the progressive fragmentation and privatisation of the railway industry,

rung der Eisenbahnindustrie, bei denen das Vertrauen zwischen allen Parteien zukünftig nicht notwendigerweise mehr vorhanden ist, oder dem Trend zu verteilten statt zentralen Architekturen. Dabei muss angemerkt werden, dass Smart Contracts nicht mit juristischen Verträgen gleichzusetzen sind, sondern es sich hierbei vielmehr um Computerprogramme oder -protokolle handelt, in denen Vertragsbedingungen hinterlegt sind sowie selbst ausgeführt und überwacht werden.

Die Implementierung einer Blockchain für das lokale Netzwerk einer Eisenbahnanlage (z. B. Stellwerk oder Zug) soll ermöglichen, im verteilten System entstehende Daten nachweislich in Echtzeit zu protokollieren. Dabei müssen aber eisenbahnspezifische Randbedingungen ausgenutzt werden, um anwendungsspezifische Anpassungen an Standard-Blockchains vorzunehmen. Dies können Änderungen bei den sogenannten Einigungsprotokollen sein. Einigungsprotokolle dienen dem Zweck, eine Wahrheit über die Daten unter Übereinstimmung aller Teilnehmer zu gewährleisten und sind in vielfältigen Ausprägungen verfügbar (z. B. die Verwendung von Einigungsprotokollen wie Proof of Authority, Proof of Work oder Proof of Stake) und haben Einfluss auf verschiedene Faktoren, wie beispielsweise Datensicherheit, Skalierbarkeit oder Geschwindigkeit in der Verarbeitung.

Hinsichtlich des Teilnehmerkreises können Public, Consortium und Private Blockchains unterschieden werden. Zusätzlich kann eine Unterscheidung in Permissioned und Permissionless Blockchains vorgenommen werden, um Lese- und Schreibberechtigungen zu verwalten.

Private Blockchains sind nur für die teilnehmenden Organisationen zugänglich. Hier wird der Einigungsprozess von autorisierten Knoten kontrolliert. Während die Schreibberechtigung also ausschließlich bei autorisierten Knoten liegt, kann die Leseberechtigung öffentlich oder auf spezifische Teilnehmer beschränkt sein. Eine solche Blockchain kann beispielsweise von einem Konsortium aus 15 Banken verwendet werden, von denen jede einen Knoten betreibt und von denen zehn jeden Block validieren müssen, damit dieser Block gültig ist. Während die Schreibberechtigung bei dieser Organisation liegt, können die Leseberechtigungen öffentlich oder beschränkt auf autorisierte Knoten sein.

Im Gegensatz zu Public Blockchains können in Private Blockchains die Regeln für den Zugriff auf Daten geändert werden. Der Wert privater Blockchains liegt vor allem in der kryptographischen Authentifizierung.

Die Unterscheidung zwischen Permissioned und Permissionless Blockchains bezieht sich auf die Erlaubnis, am Netzwerk teilzunehmen und damit Informationen der Blockchain zu lesen, die Erlaubnis, Transaktionen zu initiieren und die Erlaubnis, neue Transaktionen zu bestätigen.

In einer Permissioned Blockchain treten eine oder mehrere Autoritäten als Entscheider für die Teilnahme auf. Während Permissioned Blockchains der ursprünglichen Blockchain-Idee einer Dezentralisierung der Macht widersprechen, bieten sie auch gut regulierten Industrien wie der Eisenbahn die Chance, die Blockchain-Technologie zu nutzen. So müssen beispielsweise Lieferanten die wahre Identität ihrer Transaktionspartner kennen. Außerdem resultiert die Beschränkung der validierenden Netzwerkknoten in einer höheren Leistungsfähigkeit des Netzwerks. Für Eisenbahnanwendungen bieten sich daher vornehmlich Private Permissioned Blockchains an.

2 Das Projekt RailChain

Das Ziel von RailChain ist in erster Linie die Spezifikation und Implementierung eines Blockchain-Demonstrators für das Eisenbahnwesen, der eine Basis-Funktionalität umsetzt, auf der Echtzeitanwendungen (< 1 Sekunde Block-Zyklus-Zeit) ablaufen können sowie dessen Erprobung in einem geeigneten Testfeld.

where trust between all the parties will no longer be assured in the future. There is also a trend towards distributed rather than central architectures. It should be noted that smart contracts are not the same as legal contracts, but are rather computer programs or protocols that store, implement and monitor contractual terms.

The implementation of a Blockchain for a railway system's local network (e. g. a signal box or train) should facilitate the logging of the data generated in the distributed system in real time. However, rail-specific boundary conditions must be used to make application-specific adjustments to standard Blockchains. This can involve changes to the so-called agreement protocols. Agreement protocols serve the purpose of guaranteeing a truth about the data in accordance with the agreement of all the participants, come in a variety of forms (e. g. the use of agreement protocols such as proof of authority, proof of work or proof of stake) and influence various factors, such as data security, scalability or speed in processing.

With regard to the group of participants, a distinction can be made between public, consortium and private Blockchains. In addition, a distinction can also be made between permissioned and permissionless Blockchains for the management of read and write authorisations.

Private Blockchains are only accessible to the participating organisations. Here, the agreement process is controlled by authorised nodes. So, while the write authorisation only pertains to the authorised nodes, the read authorisation can be public or limited to specific participants. For example, such a Blockchain could be used by a consortium of 15 banks, each of which operates a node and ten of which must validate each block for this block to be valid. While the write authorisation lies with this organisation, the read authorisation can be public or restricted to authorised nodes.

In contrast to public Blockchains, the data access rules can be different in private Blockchains. The value of private Blockchains lies primarily in their cryptographic authentication.

The distinction between permissioned and permissionless Blockchains consists of the permission to participate in the network and thus read the information from the Blockchain, the permission to initiate transactions and the permission to confirm new transactions.

In a permissioned Blockchain, one or more authorities act as decision-makers with regard to participation. While permissioned Blockchains contradict the original Blockchain idea of decentralisation, they also offer well-regulated industries like railways a chance to use Blockchain technology. For example, suppliers need to know the true identity of their transaction partners. In addition, the limitation of the validating network nodes results in higher network performance. Private permissioned Blockchains are therefore particularly suitable for railway applications.

2 The RailChain project

The primary goal of RailChain is the specification and implementation of a Blockchain demonstrator for the railway industry. It will implement a basic functionality, on which real-time applications with a block cycle time of less than one second can run and which will be tested in a suitable test field.

The project is divided into three so-called Use Cases: In Use Case 1, an asset identity is developed, with which individual train components can be identified and their lifecycles and corresponding status changes can be documented (e. g. the number of braking operations performed by a brake). In Use

Das Projektvorhaben ist in drei sogenannte Use Cases unterteilt: In Use Case 1 wird eine Asset Identity entwickelt, mit der sich einzelne Komponenten eines Zuges identifizieren und ihr Lebenslauf sowie entsprechende Statusänderungen dokumentieren lassen (beispielsweise die Anzahl der Bremsvorgänge einer Bremse). In Use Case 2 ist die Implementierung eines Daten-Loggers vorgesehen, um aufzuzeigen, dass Blockchain- und Distributed Ledger-Technologien im Fahrzeug implementiert werden können. In Use Case 3 soll ein Blockchain-basiertes rechtssicheres Aufzeichnungsverfahren (im Folgenden als Juridical Blockchain Recorder (JBR)) für Eisenbahnen, das European Train Control System (ETCS) und das digitale Stellwerk (DSTW) mit Echtzeitanforderungen zum Einsatz gebracht werden. Neben der technischen Übertragbarkeit in die Bahntechnik soll zudem auch die Wirtschaftlichkeit der Blockchain-Technologie gezeigt werden.
In Bild 1 ist am Beispiel eines heute verbauten Juridical Recorders [8] erkennbar, welche weiteren Vorteile ein JBR bringen könnte. Derzeit ist eine Datenabgriff nur über eine RSR232-Schnittstelle [7] spezifiziert. Mit einem JBR könnte ein vereinfachter Zugriff auf die Daten ermöglicht werden sowie eine höhere Vertrauenswürdigkeit der Daten, da die Daten in einem JBR unveränderlich und kryptographisch gesichert abgelegt werden. Dies könnte auch den Wert der Daten steigern sowie den Einstieg in eine wirtschaftliche Verwertung der Daten ebnen.
Nach Kenntnis der Autoren ist dies der erste Anwendungsfall für Distributed-Ledger-Technologien für Echtzeit-Anwendungen im Eisenbahnbetrieb (Operational Technology).
Dieser Beitrag beschäftigt sich speziell mit den Zuverlässigkeitsanforderungen von Use Case 3, in dem eine herkömmliche Juridical Recording Unit (JRU) in Spezialhardware (in Bild 1 ist das speziell gehärtete Modul hervorgehoben) durch eine verteilte Lösung (JBR) in Standardhardware ersetzt werden. Dabei soll mit der Verteilung im Zug (z. B. vorne, mittig und hinten) eine Redundanz erreicht werden, sodass die Anforderungen an die Verlässlichkeit der einzelnen Hardwarekomponenten verringert werden können. In der Folge soll dies den Einsatz von kostengünstiger Standard-Hardware ermöglichen. In Kombination mit der Blockchain-Technologie eröffnet dieses verteilte Softwaresystem neue Möglichkeiten, z. B. bzgl. Herstellerunabhängigkeit und Telemetrie.
In diesem Beitrag soll herausgearbeitet werden, ob und unter welchen Annahmen und Randbedingungen eine JBR die Zuverlässigkeitsanforderungen der JRU erfüllen kann.

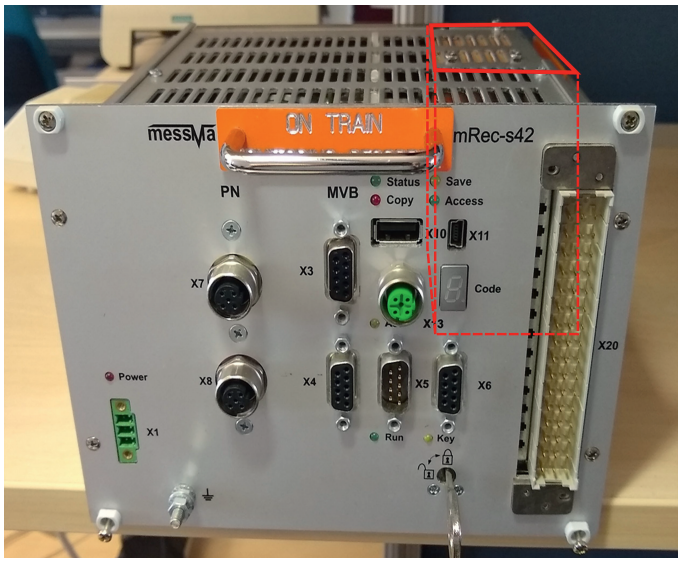

Bild 1: Beispiel für einen Juridical Recorder
Fig. 1: An example of a Juridical Recorder
Quelle / *Source*: Jens Braband

Case 2, the implementation of a data logger is provided to show that Blockchain and distributed ledger technologies can be implemented in a vehicle. A Blockchain-based, legally secure recording procedure (hereafter simply referred to as the Juridical Blockchain Recorder (JBR)) for railways, the European Train Control System (ETCS) and the digital interlocking (DSTW) with real-time requirements will be considered in Use Case 3. In addition to its technical transferability to rail technology, the cost-effectiveness of Blockchain technology should also be demonstrated.
Fig. 1 shows an example of a currently installed juridical recorder [8]. It demonstrates the further advantages that a JBR could bring. Data tapping is currently only possible via an RSR232 interface [7]. A JBR would enable simplified access to the data, as well as a higher level of data trustworthiness, since the data in the JBR would be frozen and cryptographically secured. This could also increase the value of the data and pave the way for its economic exploitation.
To the authors' knowledge, this is the first se Case for distributed ledger technologies for real-time applications in railway operations (operational technology).
This paper deals specifically with the reliability requirements of Use Case 3, in which a conventional Juridical Recording Unit (JRU) in special hardware (the especially hardened module is highlighted in fig. 1) is replaced with a distributed solution (JBR) in standard hardware. Redundancy should be achieved by means of distribution in the train (e. g. the front, middle and rear) so that the reliability requirements for the individual hardware components can be reduced. As a result, this should enable the use of inexpensive standard hardware. When combined with Blockchain technology, this distributed software system opens up new possibilities, such as independence from specific manufacturers and telemetry.
This article aims to elucidate whether and under what assumptions and boundary conditions a JBR can meet the reliability requirements of the JRU.

3 Requirements

According to the specification [4], a mean time between failures (MTBF) of 180,000 hours is required for a JRU with a mean time to repair (MTTR) of 18 hours. This corresponds to an availability A of approximately 0.9999.
It is assumed that the above MTTR only refers to the replacement time on the vehicle, as a JRU on a train is not repaired immediately, i. e. the train continues its journey despite having a defective JRU. The real time until the fault is repaired (from diagnosis) is much longer, e. g. 18 hours (for permanent operations). Assuming average locomotive operations of 16 hours per day, the true MTTR should be approximately one day, i. e. MTTR=24 hours. The described case assumes an MTTR of 18 hours in order to stay in line with the original requirements.
In the case of an accident, the JRU is especially protected against shock and fire, e. g. against fire at temperatures of up to 700° for five minutes, due to its special hardware. For the sake of simplicity, it is assumed here that the JRU protection is perfect, but that the JBR protection is not.
Since the JRU only has few, weak safety requirements, they have not been considered here. In any case, it is assumed that the tamper protection of the JBR is better than that of the JRU.
It is expected that the JBR will meet the same requirements or be even better than the JRU.

3 Anforderungen

Nach dem Lastenheft [4] wird für eine JRU eine mittlere Zeit zwischen Ausfällen (Mean Time Between Failures, MTBF) von 180 000 Stunden gefordert bei einer mittleren Fehlerbehebungszeit (Mean Time To Repair, MTTR) von 18 Stunden, dies entspricht einer Verfügbarkeit A von ca. 0,9999.
Hier wird angenommen, dass die o. a. MTTR die reine Austauschzeit auf dem Fahrzeug bezeichnet, denn die JRU auf dem Zug wird nicht sofort repariert d. h. der Zug setzt seine Fahrt trotz defekter JRU fort. Die wahre Zeit bis zum Beheben des Fehlers (seit Diagnose) beträgt wesentlich länger, z. B. 18 Stunden (bei ununterbrochenem Betrieb). Nimmt man an, dass der Zug oder die Lok durchschnittlich 16 Stunden pro Tag im Einsatz ist, dürfte die wahre MTTR in der Größenordnung von einem Tag liegen, d. h. MTTR=24 Stunden. Wir verwenden hier eine MTTR von 18 Stunden, um mit den ursprünglichen Anforderungen konform zu bleiben.
Im Fall eines Unfalls ist die JRU aufgrund ihrer Spezialhardware z. B. besonders vor Schock und Brand geschützt, z. B. gegen Feuer bis zu 700 °C über fünf Minuten. Der Einfachheit halber wird hier angenommen, dass der Schutz der JRU perfekt ist, der der JBR aber nicht.
Da die JRU nur wenige, schwache Security-Anforderungen besitzt, werden diese hier nicht betrachtet. Es wird davon ausgegangen, dass der Manipulationsschutz der JBR in jedem Fall besser ist als bei der JRU.
Die JBR soll dieselben Anforderungen erfüllen oder sogar besser sein als die JRU.

4 Fehlerszenarien

Die maßgebliche Ausfallart ist, dass die Daten der JRU nach einem meldepflichtigen Ereignis, in der Regel ein Unfall, nicht zur Verfügung stehen oder verfälscht sind.
Entscheidend ist die Suche nach gemeinsamen Ursachen, die alle Computer der JBR betreffen können. Hierbei ist zu beachten:

- Umweltbedingungen, die alle Computer, auf denen der JBR implementiert ist, nachteilig beeinflussen können. Diese werden jedoch in der Regel durch die Einhaltung der Anforderungen der EN 50125 abgedeckt. Diese Norm ist verbindlich für alle Komponenten von Schienenfahrzeugen.
- Einflüsse durch elektromagnetische Strahlung. Durch die EN 50121 werden Anforderungen hinsichtlich Emission und Strahlungsfestigkeit gestellt. In der Regel werden damit gemeinsame Einflüsse abgedeckt. Alle Komponenten von Schienenfahrzeugen müssen wiederum der EN 50121 genügen, wodurch elektromagnetische Beeinflussungen nicht weiter untersucht werden müssen.
- Mechanische Einflüsse z. B. beim Aufprall als Folge eines Unfalls
- Feuer, z. B. infolge eines Brands nach einem Unfall

Hier wurden die folgenden Szenarien durch ein Brainstorming ermittelt:

1) Die JRU fällt aus, d. h. die Daten werden nicht oder nicht mehr vollständig aufgezeichnet. Ein Unfall passiert, bevor die JRU instandgesetzt wird.
2) Ein Unfall passiert, die JRU wird so geschädigt, dass die Daten nicht oder nicht mehr vollständig zur Verfügung stehen.
3) Aufgrund einer temporären, lokalen Störung auf dem Fahrzeug, z. B. EMV, werden die Daten von der JRU verfälscht oder nicht vollständig aufgezeichnet. Ein Unfall passiert so zeitnah, dass die Daten relevant sind, aber verfälscht oder nicht vollständig aufgezeichnet werden.

4 Failure scenarios

The relevant failure type involves a case where the JRU data is not available or has been falsified after a reportable event, usually an accident.
It is crucial to find common causes that can affect all the JBR computers. The following has to be considered:

- any environmental conditions that can adversely affect all the computers, on which the JBR has been implemented. However, these are usually covered by compliance with the requirements of EN 50125. This standard is binding for all rail vehicle components.
- any influences due to electromagnetic radiation; EN 50121 sets out the requirements with regard to emissions and radiation resistance. Common influences are covered as a rule. All rail vehicle components must in turn comply with EN 50121, which means that electromagnetic influences do not need to be further investigated.
- mechanical influences, e. g. during a crash as a consequence of an accident,
- fire, e. g. as a consequence of an accident.

A brainstorming event identified the following scenarios:

1) The JRU has failed, i. e. the data is not or is no longer fully recorded. An accident happens before the JRU is repaired.
2) An accident occurs and the JRU is damaged in such a way that the data is not or is no longer completely available
3) Due to a temporary, local disturbance on the vehicle, e. g. EMC influences, the data has been falsified or has not been completely recorded by the JRU. An accident happens so promptly that the data is relevant, but it has been falsified or incompletely recorded.
4) The data has been falsified or not fully recorded in the JRU. An accident happens so promptly that the data is relevant, but has been falsified or incompletely recorded.

The scenarios relevant for this analysis have been derived from the aforementioned four. Advantage has been taken of the fact that the target for unavailability is in the order of U=0.0001, i. e. any scenarios that can only contribute a small proportion to the overall target can be neglected in the further quantitative analysis. Scenarios where the JBR outperforms the JRU can also be neglected, since only a relative comparison has been carried out.
Scenarios 1 and 2 are core scenarios and must be considered in any case. In scenario 1, the JBR is qualitatively better, while the JRU is better in scenario 2. Therefore, both scenarios must be considered.
Scenario 3 has fewer occurrences by far than scenario 1, especially since it requires an accident to occur close to an incident, usually within seconds (in scenario 1, it is within hours). Furthermore, scenario 3 has not been considered in any detail here, because the JBR is qualitatively better than the JRU.
Scenario 4 is a special variation of scenario 1, namely a specific failure mode and as such it is much less likely than scenario 1. Once again, the accident must occur promptly and the JBR is also qualitatively better than JRU in this case. Therefore, scenario 4 has not been considered in any detail here.

5 Analysis

Since the sequence of events plays a role in the scenarios, a Markov model (fig. 2) is more suitable for the modelling than a fault tree.

4) Die Daten werden in der JRU verfälscht oder nicht vollständig aufgezeichnet. Ein Unfall passiert so zeitnah, dass die Daten relevant sind, aber verfälscht oder nicht vollständig aufgezeichnet werden.

Aus diesen Szenarien werden jetzt die für diese Betrachtung relevanten Szenarien abgeleitet. Dabei wird ausgenutzt, dass das Ziel für die Unverfügbarkeit in der Größenordnung von U=0,0001 liegt, d. h. alles Szenarien, die von der Größenordnung her nur einen geringen Bruchteil zum Ziel beitragen können, können in der weiteren quantitativen Betrachtung vernachlässigt werden. Auch Szenarien, bei denen die JBR besser als die JRU ist, dürfen vernachlässigt werden, da nur ein relativer Vergleich angestrebt wird.

Die Szenarien 1 und 2 sind Kernszenarien und müssen in jedem Fall betrachtet werden. In Szenario 1 ist die JBR qualitativ besser, in Szenario 2 die JRU. Deswegen müssen beide Szenarien betrachtet werden.

Szenario 3 ist um Größenordnungen seltener als Szenario 1, insbesondere, da ein Unfall zeitnah zu einer Störung, in der Regel innerhalb von Sekunden, auftreten muss (bei Szenario 1 innerhalb von Stunden). Da außerdem die JBR hier qualitativ besser ist als die JRU, wird das Szenario 3 hier nicht detailliert betrachtet.

Szenario 4 ist ein Spezialfall von Szenario 1, nämlich ein spezifischer Ausfallmodus d. h. wesentlich unwahrscheinlicher als Szenario 1. Der Unfall muss wieder zeitnah auftreten und die JBR ist hier wieder qualitativ besser als JRU. Daher wird auch das Szenario 4 hier nicht detailliert betrachtet.

5 Analyse

Da schon bei den Szenarien die Reihenfolge von Ereignissen eine Rolle spielt, bietet sich hier ein Markov-Modell (Bild 2) zur Modellierung eher an als ein Fehlerbaum.

Man erkennt schon an dem einfachen Modell, dass es zwei unabhängige Beiträge zur Ereignisrate gibt (und zwar nach den Szenarien nummeriert):

$$\lambda_1 \approx \lambda_U \frac{MTTR}{MTBF}$$

und

$$\lambda_2 \approx \lambda_U P_V$$

Die erste Erkenntnis aus der Analyse ist, dass für den relativen Vergleich die Unfallrate λ_U nicht relevant ist, da die Art der Aufzeichnung keinen Einfluss auf diese hat.

Es soll angenommen werden, dass bei der JBR keine Spezialhardware eingesetzt wird, sondern die Funktionalität auf normalen, fahrzeugtauglichen Rechnern ausgeführt wird, im Idealfall als zusätzliche Funktionalität auf Rechnern, die schon vorhanden sind. Daher wird angenommen, dass die Funktionalität auf N Rechnern ausgeführt wird, die aber im ersten Schritt von der Zuverlässigkeit her als identisch angenommen werden. Konservativ wird angenommen, dass MTBF =20 000 Stunden gilt (dies entspricht einer Ausfallrate von ca. 5 10^{-5}/h, zur Plausibilisierung siehe [3], hier wird ein Wert von 2,3 10^{-5}/h für „military" angegeben), d. h. jeder Rechner würde je nach Betriebsbeanspruchung ca. alle zwei Jahre ausfallen. Bei der MTTR wird konservativ angenommen, dass diese genauso wie bei der JRU gleich 18 Stunden ist. Auch hier wird es Rechner geben, die aufgrund ihrer betrieblichen Funktion wesentlich schneller instandgesetzt werden müssen. Für die Unverfügbarkeit der JBR gilt dann im Szenario 1

$$U_1^V = U^N$$

This simple model clearly shows that there are two independent contributions to the event rate (numbered according to the different scenarios):

$$\lambda_1 \approx \lambda_U \frac{MTTR}{MTBF}$$

and

$$\lambda_2 \approx \lambda_U P_V$$

The first finding of the analysis is that the accident rate λ_U is not relevant for a relative comparison since the manner of recoding does not influence the recording itself.

It is to be assumed that no special hardware is used with the JBR, but that the functionality is executed on normal, vehicle-compatible computers, ideally as an additional functionality on computers that already exist. Therefore, it is assumed that the functionality is executed on N computers, which are assumed in the first step to be identical regarding their reliability. It is conservatively assumed that MTBF =20,000 h (this corresponds to a failure rate of approx. 5 10^{-5}/h; see [3], where a value of 2.3 10^{-5}/h is given for "military", for the plausibility check), i. e. each computer would fail approximately every two years depending on the operating load. The MTTR is conservatively assumed to be 18 hours, just like the JRU. Here, too, there will be computers that will have to be repaired much faster due to their operating functions. The following applies for the unavailability of the JBR in scenario 1

$$U_1^V = U^N$$

because the 1-out-of-N system present here for the JBR means that all the components must be unavailable in order to cause the unavailability of the entire system. U = 9 10^{-4} applies under the aforementioned assumption and N=2 results in an unavailability of 8.1 10^{-7} for the JBR, which is at least a factor of 100 better than the JRU for scenario 1.

With regard to scenario 2, the probability of total data loss after an accident must be considered for the JBR, i. e. all the N JBR units are destroyed. For the JBR solution to be at least as good as the JRU, this probability must be in the order of 0.0001, i. e. all N JBR are destroyed in one or two accidents out of 10,000. Assuming that the JBR are not all placed in one place on the vehicle, consideration can be limited to the fact that the whole vehicle will be destroyed in the accident.

Four participants are necessary for a planned fault-secure agreement protocol (also called "Byzantine Fault Tolerant"). Therefore, we will now assume the existence of four independent computers in our further considerations. However, we will initially only consider the pure reliability requirements explicitly and not the additional security requirements, which would quasi-require a 3-out-of-4 system, while a 1-out-of-4 system is sufficient from a purely availability perspective. However, even with an availability of 0.996 for a single component, the availability target could still be reached, so that there are no practical restrictions.

6 The statistical approach

The UIC reported a total of 4017 significant accidents for 2018, i. e. accidents in which at least one train was in motion and at least one fatality or considerable material damage resulted. Although this fig. also includes purely personal injuries, there is of course a high number of unreported accidents that do not result in serious personal injury or significant material damage. How-

denn bei dem hier bei der JBR vorliegenden 1-von-N-System müssen alle Komponenten unverfügbar sein, damit das Gesamtsystem unverfügbar ist. Unter der obigen Annahme gilt $U = 9\ 10^{-4}$, und schon für N = 2 ergibt sich mit $8{,}1\ 10^{-7}$ eine Unverfügbarkeit für die JBR, die für Szenario 1 um mindestens einen Faktor 100 besser ist als die JRU.

Für Szenario 2 muss für die JBR die Wahrscheinlichkeit eines totalen Datenverlustes nach einem Unfall betrachtet werden, d. h. alle N JBR werden zerstört. Damit die JBR-Lösung mindestens genauso gut ist wie die JRU, muss diese Wahrscheinlichkeit in der Größenordnung 0,0001 liegen, d. h. in ein oder zwei Unfällen aus 10 000 Unfällen werden alle N JBR zerstört. Unter der Annahme, dass die JBR nicht an einer Stelle des Fahrzeugs, sondern über die Länge verteilt platziert werden, kann man die Betrachtung darauf beschränken, dass bei dem Unfall das gesamte Fahrzeug zerstört wird.

Für das geplante gegen Fehler sicherere (auch „Byzantine Fault Tolerant" genannte) Einigungsprotokoll sind vier Teilnehmer nötig, daher gehen wir bei unseren Betrachtungen von vier JBR-Einheiten aus. Allerdings betrachten wir hier erstmal nur die reinen Zuverlässigkeitsanforderungen explizit, nicht die sich aus der Security zusätzlich ergebenden Anforderungen, die quasi ein 3-von-4-System verlangen würden, während aus reiner Verfügbarkeits-Sicht ein 1-von-4-System ausreicht. Aber schon bei einer Verfügbarkeit von 0.996 für eine einzelne Komponente

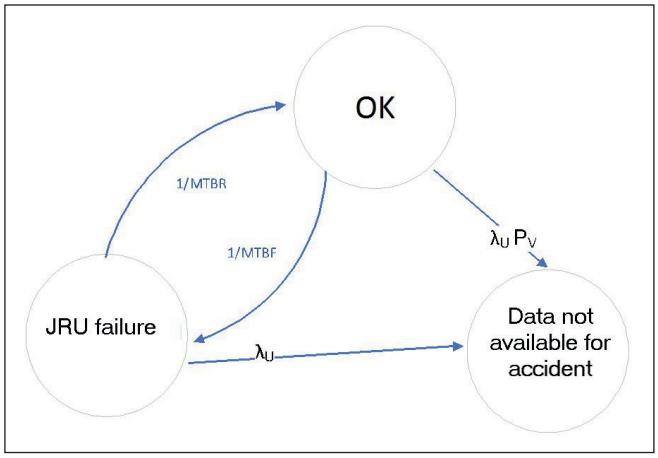

Bild 2: Markov-Modell
Fig. 2: The Markov model
Quelle / *Source*: eigene Darstellung / *own illustration*

ever, it may be assumed that the evaluation of the recorder data would also have been necessary or useful in many other cases. The European Railway Agency (ERA) reported 1789 significant accidents for the EU in 2016. This is in correlation with the UIC figures for the EU. About 10,000 trains in the EU have been equipped with ETCS, but the goal is to reach full equipment in the EU.

Unfallszenario	Anteil des Szenarios an allen Unfällen	Anteil von Unfällen mit Toten	Anteil des Szenarios mit tödlichem Ausgang von allen Unfällen
Entgleisung: Anteil 2,5 %	2,50 %	28,7 %	0,72 %
Zusammenstoß mit anderem Zug	0,50 %	63,6 %	0,32 %
Feuer	0,60 %	0 %	0 %
Summe			1,04 %

Tab. 1: Anteile von Unfallszenarien

Accident scenario	Share of the scenario in all accidents	Share of accidents with fatalities	Share of fatal scenario of all accidents
Derailment: a 2.5% rate	2,50 %	28,7 %	0,72 %
Collision with another train	0,50 %	63,6 %	0,32 %
Fire	0,60 %	0 %	0 %
Total			1,04 %

Tab. 1: Accident scenario rates

könnte auch dann noch das Verfügbarkeitsziel erreicht werden, sodass sich auch hier keine praxisrelevanten Einschränkungen ergeben.

6 Statistischer Ansatz

Die UIC berichtet für 2018 insgesamt 4017 signifikante Unfälle, das sind Unfälle, bei denen mindestens ein Zug in Bewegung ist und mindestens ein Unfallopfer oder hoher Sachschaden resultiert. Zwar sind hier auch reine Personenunfälle enthalten, allerdings gibt es natürlich eine hohe Dunkelziffer von Unfällen, die ohne ernsthafte Personenschäden oder hohe Sachschäden ausgehen. Aber es darf angenommen werden, dass auch in vielen weiteren Fällen die Auswertung der Rekorderdaten notwendig bzw. sinnvoll gewesen wäre.
Die europäische Eisenbahnagentur (ERA) berichtet für die EU für 2016 1789 signifikante Unfälle. Dies stimmt gut mit den UIC-Zahlen für die EU überein. Etwa 10 000 Züge sind in der EU mit ETCS ausgestattet, aber das Ziel ist eine Vollausrüstung in der EU.
Geht man konservativ vor, so kann man annehmen, dass folgende Anteile der durch die UIC berichteten Unfälle [1] zu einer Zerstörung der gesamten Lok bzw. des Zuges führen:

- Entgleisung: Anteil 2,5 %
- Zusammenstoß mit anderem Zug: Anteil 0,5 %
- Feuer: Anteil 0,6 %,

d. h. 3,6 % aller Unfälle haben das Potenzial, im ungünstigsten Fall zur Zerstörung aller JBR zu führen.
Diese Betrachtungen lassen sich fortführen. Nicht jeder der genannten Unfälle führt nun zu einer schwerwiegenden Zerstörung der Lokomotive. Gehen wir davon aus, dass bei Unfällen, die schwerwiegende Zerstörungen an der Lokomotive oder dem Triebzug hervorrufen können, mindestens ein Toter auftreten muss. Wir gehen davon aus, dass derart schwerwiegende Unfälle nötig sind, um den Speicherbaustein des betreffenden Computers zu zerstören. Ein Speicherbaubaustein ist ohne Zweifel robuster als ein Mensch.
Tab. 1 gibt die Berechnungen wieder.
Hierzu ist anzumerken:

- Crashsituationen: Beim Crash von Schienenfahrzeugen können durchaus zwei Computer zerstört werden. In der Regel ist ein crash-sicherer Ort in der Mitte der Lokomotive oder in der Mitte des Triebzuges. Man müsste hier die Computer mit entsprechendem Abstand installieren. Bei Triebzügen ist dies möglich, sodass man ohne weitere Analyse davon aus-

If one takes a conservative approach, it can be assumed that the following rates of accidents [1] reported by the UIC lead to the destruction of the entire locomotive or train

- derailment: 2.5 %
- collision with another train: 0.5 %.
- fire: 0.6 %,

i. e. 3.6 % of all accidents have the potential to lead to the destruction of all the JBRs in the worst case scenario.
These considerations can be further elaborated. However, not all of the accidents mentioned above lead to the significant destruction of the locomotive. Let us assume that accidents that can cause serious damage to the locomotive or multiple units must result in at least one death.
We can assume that such serious accidents are necessary to destroy the memory module of the computer in question. There is no doubt that a memory chip is more robust than a human being.
Tab. 1 shows the calculations.
It should be noted in this respect:

- Crash situations. Two computers can be destroyed in a rail vehicle crash. As a rule, the middle / centre of the locomotive or the middle / centre of the multiple unit is a crash-safe place. The computers would have to be installed at an appropriate distance. This is possible with multiple units, so it can be assumed without any further analysis that not all the computers will be destroyed in crashes. It is difficult to assess the extent to which not all the computers can be damaged by a severe crash in individual locomotives.
- Nothing has been calculated with regard to the case of fire, as no deaths from fire were reported in the sample. In the case of multiple units, one of the four computers will always survive with a probability close to one. It should also be noted that fire prevention and, in some cases, firefighting measures are implemented in modern locomotives – and they are also equipped with ETCS.

This results in a probability of about 1 % that several computers will be affected.
This figure was compared to the proportion of serious accidents (derailments, collisions, fires or construction machinery or equipment impacts resulting in damage exceeding EUR 150,000 or at least one fatality) at Deutsche Bahn AG (DB). The latter evaluation resulted in a probability of 2.66 10^{-3}. This calculation thus supports the assumptions made above.
We now assume that there will be two pairs of computers located at the ends of the train.
The probability that not only the computer pair at one end, but also the computer pair at the other end will be affected by any cata-

gehen kann, dass bei Crashs nicht alle vier Computer zerstört werden. Inwiefern bei einzelnen Lokomotiven durch starken Crash nicht doch alle Computer beschädigt werden können, lässt sich schwer einschätzen.
- Bei Feuer wurde kein Beitrag berechnet, da in der Stichprobe keine Toten durch Feuer berichtet wurden. Im Fall von Triebzügen wird mit einer Wahrscheinlichkeit nahe Eins immer einer der vier Computer überleben. Zudem ist festzustellen, dass in modernen Lokomotiven – und diese sind mit ETCS ausgerüstet – Brandverhütungs- und teilweise -bekämpfungsmaßnahmen implementiert sind.

Hieraus ergibt sich eine Wahrscheinlichkeit von ca. 1 %, dass mehrere Computer betroffen sind.
Dieser Wert wurde mit dem Anteil schwerer Unfälle (Entgleisungen, Zusammenstöße, Brand, Aufprall Baumaschine bzw. Baugerät mit Schaden über 150 000 EUR bzw. mindestens einem Toten) bei der Deutschen Bahn AG (DB) verglichen. Aus der letzteren Auswertung ergab sich eine Wahrscheinlichkeit von 2,66 10^{-3}.
Damit stützt diese Berechnung die oben gemachten Annahmen.
Allerdings gibt es auch noch weitere Faktoren, die die Verfügbarkeit der JBR-Lösung noch verbessern würden, allerdings hier numerisch nicht mit betrachtet wurden: Z. B. kann man bei der JBR-Lösung die Daten zusätzlich an der Streckenseite spiegeln, z. B. immer, wenn eine Breitbandverbindung zur Verfügung steht. Oder man kann die aktuellen Daten immer an die Streckenseite übertragen, wenn die JBR eine außergewöhnliche Betriebssituation erkennt, z. B. eine Notbremsung.

7 Diskussion und Zusammenfassung

Die durchgeführte Abschätzung hat gezeigt, dass es durchaus möglich ist mit einem JBR (Juridical Blockchain Recorder), der aus vier verteilten Computern besteht, auf einem Eisenbahnfahrzeug eine Verfügbarkeit von 10^{-4} bezogen auf einen Unfall zu erreichen. Die Berechnung ist eine Abschätzung und bedarf vor der Implementierung des Konzeptes noch einer weitergehenden Prüfung in Bezug auf Crashaspekte oder Brandschutzaspekte. Bei einer Anwendung auf der Infrastrukturseite, z. B. im Stellwerk, wo diese Aspekte keine Rolle spielen, kann man die JBR-Funktionalität mit zwei Computern umsetzen.
Was in den vorstehenden Betrachtungen außen vor geblieben ist, ist die wachsende Komplexität und dadurch ggf. weitere potenzielle Fehlerursachen sowie auch die zusätzliche Kommunikationslast auf dem Fahrzeugbus. Dadurch könnte zum einen die Zuverlässigkeit verringert werden, auch wenn dies in die klassischen Berechnungen der Zuverlässigkeit so nicht eingeht. Andererseits muss man allerdings auch einräumen, dass ein JBR wohl eher in zukünftigen Fahrzeugarchitekturen oder modernen Stellwerksarchitekturen verwirklicht werden wird anstatt als Nachrüstlösung für bestehende Systeme.
Insgesamt kann man feststellen, dass auch in diesem Fall der Digitalisierung nichts im Wege steht, wenn rechtzeitig Architekturkonzepte erstellt und Zuverlässigkeitsanalysen aufeinander abgestimmt werden.

8 Danksagung

Die Autoren bedanken sich beim RailChain Projektteam für die Unterstützung und die zahlreichen technischen Diskussionen, insbesondere aber bei Rainer Beck (Deutsche Bahn AG) für den Abgleich der Abschätzungen mit statistischen Ereignisdaten der Deutschen Bahn AG. ■

strophic accidents is thus assumed to be 1 % * 1 %, i. e. 10^{-4}, and it has thus achieved the required value.
It should be noted that this calculation is an estimate and not a strict proof. This would require further investigation.

7 Conclusion

The performed assessment has shown that it is possible to achieve an availability of 10^{-4} in relation to an accident with a JBR (Juridical Blockchain Recorder) consisting of four distributed computers on a railway vehicle. The calculation is an estimate and requires further elaboration in terms of crash aspects or fire protection aspects before the concept is implemented. When used on the infrastructure side, e. g. in an interlocking, where these aspects do not play a role, the JBR functionality can be implemented with just two computers.
The increasing complexity has been omitted from the considerations above. As a result, further potential causes of errors, as well as the additional communication load on the vehicle bus, have not been considered. On the one hand side, this could reduce the reliability, even if this is not included in classic reliability calculations. On the other hand side, however, one must also admit that a JBR will probably be implemented in future vehicle architectures or modern interlocking architectures rather than as a retrofit solution for existing systems.
Finally, it can also be concluded that digitalisation does not present an obstacle in this case, provided the architectural concepts are created in good time and the reliability analyses are coordinated with them.

8 Acknowledgement

The authors would like to thank the RailChain project team for their support and numerous technical discussions, but especially Rainer Beck (Deutsche Bahn AG) for comparing the estimates with the statistical event data from Deutsche Bahn AG. ■

LITERATUR | LITERATURE

[1] UIC: Safety Report: Significant accidents 2018, , 2019, https://safetydb.uic.org/IMG/pdf/sdb_report_2019_public.pdf
[2] European Union Agency for Railways Railway Safety and Interoperability Report in the EU 2018
[3] NPRD: Non-electronic Parts Reliability Handbook, 2011
[4] Deutsche Bahn AG: Teillastenheft 4 ETCS Fahrzeug-Ausrüstung, Anhang 2 - Juridical Recording Unit (JRU) Version 2.0, 08.07.2011
[5] Narayanan, A. et al.: Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016
[6] Kuperberg, M.; Kindler, D.; Jeschke, S.: Are Smart Contracts and Blockchains SuiTab. for Decentralized Railway Control? Preprint, arXiv:1901.06236, 2019
[7] UNISIG: FFFIS Juridical Recorder-Downloading tool, SUBSET-027, Issue 2.3.0, 2009
[8] messMa: Datenrecorder mRec-s42, Datenblatt, Ausgabe V.02, 2012

AUTOREN | AUTHORS

Prof. Dr. Jens Braband
Principal Key Expert
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: jens.braband@siemens.com

Hendrik Schäbe
Principal Assessor RAMS
TÜV Rheinland InterTraffic GmbH
Anschrift / *Address*: Am Grauen Stein, D-51105 Köln
E-Mail: schaebe@de.tuv.com