# Blockchain Technology for Emergency Response

Carsten Siemon
Austrian Institute of Management
carsten@siem-on-line.de

David Rueckel
Johannes Kepler University Linz
david.rueckel@jku.at

Barbara Krumay
Johannes Kepler University Linz
barbara.krumay@jku.at

## Abstract

*As unforeseen situations, emergencies threaten the environment, property, and people's lives. Large emergencies are characterized by the demand for coordination of a variety of actors, such as civil defense or disaster relief. Communication and information exchange are crucial for coordination. Therefore, a solid, stable communication infrastructure is among the crucial factors for emergency response. New technologies that seem to ensure trustworthy communication must be evaluated constantly. Blockchain technology is widely applied in a broad variety of contexts and is commonly known for its decentralized and distributed governance. This is the motivation for the design and evaluation of a framework for the adoption of blockchain technology in the case of emergency response following a design science approach. Evaluation of the artifact using a specific evaluation framework clearly indicates the suitability of the case for application of blockchain technology.*

## 1. Introduction

Blockchain is commonly seen as seminal technology with the potential to substantially change business models, business processes, and the economy as a whole [6]. Regardless of the discussion of whether blockchain technology can lead to disruptive shifts in a market, in enterprise settings, the application is an intensely researched topic in information systems (IS) research [43]. Blockchain technology is widely applied in a broad variety of contexts, from typical IS tasks, such as enterprise modeling [16] to rather specialized topics, such as financial fraud [22]. This indicates blockchain is both a technical and economical innovation [31]. The literature widely confirms the assumption that one crucial benefit of the application of blockchain results from the decentralized, distributed governance that is enabled by its fundamental concept. This may lead to an increase of objectivity and trust [6]. Trust is inevitable for people and organizations in situations associated with the loss of trustworthy authorities. Local, national, or global cases of emergency may lead to such situations, as common and established infrastructures may be temporarily or even permanently unavailable or untrustworthy.

As communication and data interchange are crucial in cases of emergency (e.g., for alerting, dispatching, and localizing incident resources), the design and evaluation of concepts for the application of cutting-edge technologies is indispensable. Thus, we derive the aim of this study as designing and evaluating a framework for the adoption of blockchain technology in the case of emergency response.

## 2. State of the field

Emergencies are unforeseen situations caused by harmful events or disasters that threaten the environment, property, and people's lives. While smaller emergencies are managed by public or private or for-profit emergency services, larger emergencies are also handled by a variety of actors, such as civil defense, disaster relief, and other government and non-governmental organizations. Regardless of the size and whether the emergencies occur completely without warning or are foreseeable and expected, emergencies can only be managed if all actors involved in the response cooperate and react in an efficient and coordinated manner. Therefore, the accurate and optimal provision of information is an indispensable prerequisite because the decisions of the individual actors can have far-reaching effects [35, 38]. The diversity of skills, abilities, and knowledge that individual actors provide is essential for complete emergency management. However, this diversity is also one of the obstacles, if, in the event of serious emergencies, all efforts must be directed toward a common goal [52]. The source of diversity is that each actor has its own individual system for leading, coordinating, and directing emergency forces [30]. This approach may be valuable for the

URI: https://hdl.handle.net/10125/63814
978-0-9981331-3-3

individual actor, but it leads to considerable drawbacks in the cooperating and networked operation of command and control center systems [36]. Accurate, accessible, and timely information is essential for the coordination of emergencies. For an effective response, the actors share their information at strategic, tactical, and operational levels. In concrete terms, information on the number of victims and their injuries along with important status information, such as the availability of incident forces and incident resources, is shared. Whereby, during the emergency, the status and configuration of a multitude of elements can change in a highly dynamic manner [7, 27]. In addition, emergencies always have a geographical reference. Accordingly, actors use geo-IS for fast and reliable visualization of situational information before, during, and after the emergency [30, 55]. To assess the situation and make informed decisions, actors must process a large amount of geographical information based on shared location maps. This helps to effectively develop a collective situation awareness [9, 42].

To coordinate emergencies, for decades, voice communication, analog mobile radios, and paper processes have been used. These methods are robust, but no longer meet today's requirements. New services and applications are enabled by emerging and already-established digital standards. These must be carefully checked for interoperability and robustness [1]. Interoperability demands closely coordinated processes and activities for operation and communication, and must equally address the political, legal, semantic, organizational, and technical levels [2, 29]. The cooperation between the involved actors is highly determined by legal regulations regarding notification and documentation duties [42] on top of technical aspects. Communication functions must be provided in very challenging and complex environments. The effects of catastrophic events often impair and destroy critical infrastructures, such as energy and communications [5, 7]. In the context of emergency response, hastily formed relief networks have a shared information and communication space in which the different communities implement, plan, and commit themselves to specific operations [47].

In addition, visual information in shared information spaces improves communication efficiency and increases the knowledge of the task structure and the situational awareness, especially when solving complex problems [28, 42]. However, cooperation in emergencies also means that individual organizations share their resources and subordinate their individual objectives to a common predominant goal. If monitoring functions are not to become an administrative burden, a high degree of trust is required [49]. Therefore, a crucial precondition for an interpersonal and interorganizational information exchange and cooperation is trust. Thus, the information providers in an interorganizational network will not exchange their messages without guarantee of classical information security features [25, 29, 47].

The literature on interoperability solutions in emergency management shows that distributed database technologies are used to increase availability. In combination with peer-to-peer network technologies, a distributed and scalable information space is created in which the workload and redundancy are equally configurable [1, 52]. However, the approaches do not consider how to add ad hoc new actors with their incident forces and incident resources into the interoperability systems and how to build and sustain trust between all participants. A blockchain is basically a distributed database of data records and, accordingly, a decentralized data structure [10, 12]. The blockchain technology combines several existing technologies, such as distributed ledger technology, public key encryption, hashing, and consensus protocols [46]. Technically, a regularly synchronized copy of the entire database is stored on each node of the blockchain peer-to-peer network. The database itself is organized into smaller timestamped datasets, called blocks, containing header data and multiple transactions. Whereby each block header contains a hash value of the previous block, a hash value of the included transactions as well as a random number. By referencing the hash value of the previous block, a chain of blocks is formed. Since changing a block also changes its hash value, this concept ensures the integrity of the entire blockchain back to the first block in the chain. As a result, hashing can be used by all participants to transparently verify the integrity of the entire blockchain [11, 39, 53]. By using asymmetric encryption, the attribute's authentication, integrity, and non-repudiation are added to the blockchain network [33].

Until the advent of blockchain technology ledgers always remained centralized [13]. For decentralization and distribution of the ledger various distributed consensus mechanisms have been developed with different advantages and disadvantages in terms of transaction speed, energy efficiency, scalability, immutability, and tamper resistance, depending on the selected access model to the blockchain network [31, 50]. As a specific technology for digital currencies, the blockchain solves the problem of double spending in peer-to-peer networks [37]. As a general technology, the

blockchain is a disruptive technology and enables plentiful applications that could affect the entire economy [23, 33]. With the blockchain, new forms of distributed software architectures can be developed [46]. By eliminating the constant need for actively mediated data synchronization and competing access control, the blockchain provides efficiency gains for enterprise and industrial systems based on existing structures. Furthermore, the blockchain is a censorship and tamper-proofed digital and distributed platform with the ability to establish trust without intermediaries [19]. As a decentralized technology, the blockchain enables distributed autonomous organizations (DAO) and distributed collaborative organizations (DCO) via smart contracts [13]. If the blockchain technology unfolds the expectations placed in it, the technology can create a new level of objectivity and trust in a decentralized digital world, where no one has the full control and power to deceive others or to manipulate past or current events [6]. As a specific technology for digital currencies, the blockchain implements a simple replicated state machine model that moves virtual coins from one address to another [14].

Today's blockchains integrate user-defined states and Turing complete state machine models [24] that can solve any general purpose problem. Generally, today's blockchains are distributed and highly configurable application platforms, including adjustable consensus mechanisms on top of digital smart contracts, which are programmed in high-level languages and executed inside containers on all nodes of the network [14, 24]. The structure of the blockchain has two significant benefits. All questions regarding error tolerance and parallelism are contained in the consensus protocol, and any type of data structure can be implemented regardless of its complexity [19]. According to Brewer's theorem, a distributed data structure can only guarantee two of the three properties at the same time: "consistency," "availability," and "partition tolerance" [17]. Thus, the different configurations and in high level languages programmed smart contracts define not only the layout of the blockchain but also the integration possibilities and application options. Different configurations can enable the blockchain to interact with other blockchains and with third-party systems [46]. As far as the literature is concerned, blockchain technology seems to be a promising solution to overcome the challenges in emergency response.

Even though this assumption can be derived, the application of blockchain technology in emergency response is – to the best of our knowledge - rarely discussed in IS scientific literature.

## 3. Methodology

As the aim of this study is to provide a framework for adopting blockchain technology for emergency response, we developed a corresponding artifact. The artifact development relies on a design science research (DSR) approach [18, 21, 41].

Following the idea of a rigorous application of DSR, we first determine the problem relevance and further adhere to the design as a search process and as an artifact [20]. Next, a decent evaluation of the design leads to the final artifact, which contributes to the research and to the application in the real world [20]. The developed artifact (framework) is tested regarding validity, utility, and reliability [21]. The development of the artifact itself is based on the six steps of Peffers et al. [41] and integrates different sources for design, development, testing, evaluation, and iterations, as shown in other DSR studies [3, 8].

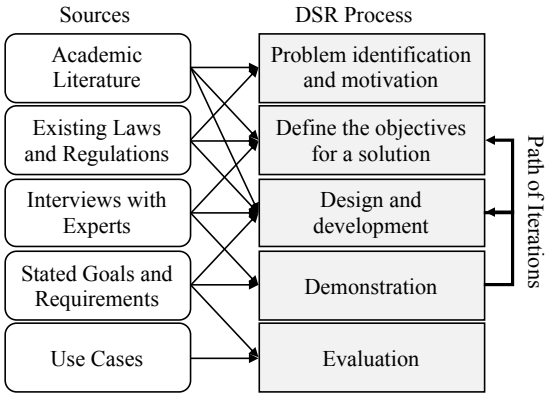


**Figure 1. Steps in DSR based on [41] and sources used to inform steps 1–5**

We describe the problem definition and objectives first, followed by the design and development process, as suggested by Gregor and Hevner [18]. After this, the artifact is described in detail. Figure 1describes the use of data sources in the DSR process (steps 1 to 5) according to Peffers et al. [41].

### 3.1 Problem identification, motivation, and objectives for solution

An artifact (as defined in DSR) by its nature solves real-world problems, in particular fulfilling business needs, and is based on a solid theoretical foundation and correctly applied research methods [21]. In this study, the artifact resembles a framework demonstrating how blockchain technology can be applied in emergency response. Emergency response means reacting quickly and reliably in situations provoked by unforeseen events, which threaten

environment, property, and people's lives [52]. According to the literature, an appropriate emergency response is influenced by the severity of the event and the skills and knowledge of the people involved [52]. However, other factors, such as the coordination between emergency response teams with different IS installed, the heterogeneity of the data, and the affected or destroyed infrastructure, may complicate the situation [48, 52]. Although technology is already in use to support emergency response, in particular in the dispatch center, cooperation and coordination in an emergency situation require high availability, which can be established via distributed databases and peer-to-peer networks [1, 52]. A more current approach of distributed information provision is the blockchain technology, based on the idea of a distributed ledger [19]. The objective of the artifact presented in this study is to show how blockchain technology can be used for emergency response to overcome limiting factors, such as the incompleteness of information and data heterogeneity, to name just a few.

## 3.2 Artifact design and development

Based on problem relevance and the general defined objectives, information was drawn from the academic literature, existing laws and regulations, and interviews with experts to gain new insight for design and development. In addition, requirements engineering – often used in software development – was applied to further structure the approach, particularly the results from the interviews. For the semi-structured interviews with experts, an interview guideline was developed, covering the technical and functional aspects. All interviews were recorded, transcribed, and analyzed based on a content analysis approach, relying on coding techniques (open coding and axial coding), as proposed for the grounded theory approach [45]. Experts were defined as people having expert knowledge in the corresponding field, long-term experience in emergency response, and practical knowledge regarding technical issues related to collaboration and coordination. Therefore, we approached a fire department in a city (approx. 750,000 inhabitants) in central Europe. The fire department consists of about 1,200 employees and is among the six biggest fire departments in the country. All five interviewees are related to this fire brigade on various hierarchical levels (see Table 1). All interviews were conducted in a calm, neutral environment. The average interview time was 50 min. One follow-up interview was conducted with I4 to clarify some information, which lasted about 30 min.

**Table 1. Description of interviewees**

| No | Job Title | In Job (since) |
|---|---|---|
| I1 | Chief of Department Fire & Rescue Service | 1993 |
| I2 | Chief Information Officer | 2009 |
| I3 | Chief of Emergency Service Command | 2010 |
| I4 | Supervisor of Central Dispatch Center | 1994 |
| I5 | Chief of Disaster Prevention & Planning Section | 2008 |

Since in-depth blockchain knowledge could not be assumed among the experts, the interview started with a general introduction, presenting the basics of blockchain technology. To achieve trust and acceptance for the technology, this part endorsed blockchain technology as a solid, valid, and stable approach to improve certain issues evolving from the current technologies in emergency response. This was necessary to ensure that the interviewees did not repudiate the technology but perceived it as a possible solution. In general, the interviews revealed different goals and requirements regarding IS related to emergency response. Besides the technological and functional aspects, organizational (e.g., stakeholders in general, partners, internal communication, interfaces, and overlaps) aspects were mentioned. In addition, they addressed issues, such as not having a leading system (information must be collected via phone), chronological documentation of events (to avoid manipulation of timestamps and acknowledgment), missing validity check of information ("I would rather work with incomplete information compared to invalid information" I3), the possibility to address a specific node (e.g., specialized forces for earthquakes) in the communication network, and standardized communication policies (syntax and semantics). Furthermore, topics such as privacy, confidentiality, and integrity of data were mentioned. One interviewee (I5) referred to the usability and urge to have a standardized and intuitive design of the graphical user interface to increase acceptance. However, all interviewees agreed that "one system for all organizations involved is not possible" (I2), as the organizations already have invested in systems. Therefore, having interoperability in terms of the exchange of information among various platforms and systems has been expressed as a principal issue. Interoperability consequently means access from everywhere that is independent of a specific system or platform. Although not discussed in the interviews in-depth, geo-positioning is among the critical

requirements for a solid emergency response. These organizational issues strongly influence technological and functional requirements and goals. Based on the interviews and the literature, five goals have been defined. Goal 1 (G1) states that a solution must support intra-organizational and interorganizational interoperability and must be also suitable for the seamless integration of all necessary communication partners beyond the boundaries of federalism (G1.1). Furthermore, the solution must consider that the individual partners use different management structures and that the organizational and professional cultures of the distinct emergency organizations differ (G1.2). Goal 2 (G2) defines the exchange of geospatial data for the purpose of semi-automated dispatching and alerting of incident equipment from partners (G.2.1) and the broadcast of general requirement requests to the community to cover the need for additional resources (G2.2). Goal 3 (G3) targets the exchange of incident and situation information on the damage event and damage defense in the emergency scene (G3.1), the spatial management of areas like mission, staging, and collecting or assembling areas (G3.2), and the personal data (G3.3) with the objective to develop a collective unambiguous situational awareness (G3.4). Goal 4 (G4) covers the automation of communication between partners with the objectives to increase the speed of information processing in the command and control center (G4.1), to reduce the information gaps between actual situations and the information at hand (G4.2), and to increase human resources for coordinating situations and scenes of incidents (G4.3). Finally, Goal 5 (G5) targets the establishment of a crisis-proof, failsafe, and trustworthy solution for interorganizational collaboration, which is applicable for all types of incidents (G5.1), including for major emergencies (G5.2) with the ability to exchange confidential information (G5.3), for planning and obligation (G5.4), for legally binding liabilities (G5.5), for considering the vertical and horizontal separation of powers (G5.6), and for creating data and information that can be used before a court (G5.7). In addition, six technical and functional requirements were elaborated. Requirement 1 (R1) covers an interface solution between command and control center systems to establish interoperability, including identity and access management (R1.1), appropriate scalability (R1.2), and the speed of the transaction (R1.3). Requirement 2 (R2) targets control of the information flow, addressing specific participants (R2.1) and establishing information channels between interorganizational and intra-organizational participants (R2.2). Requirement 3 (R3) describes the exchange and storage of information that is characterized by high availability (R3.1); is encrypted, consistent, and robust against manipulation (R3.2); is time stamped, documented, and recorded (R3.3); and is legally compliant (R3.4). Requirement 4 (R4) covers the exchange of information with geospatial objects (i.e., context information (R4.1), status messages (coded or plain) (R4.2), or remote orders (coded or plain) (R4.3)). Requirement 5 (R5) includes an information exchange with geospatial references for dispatching and alerting incident forces and incident resources, transmission of the unique individual short subscriber identity (ISSI) of the European TETRA digital radio system (R5.1), transmission of national radio status codes to determine the incident resource availability (R5.2), and transmission of additional characterizing information on the incident resources (R5.3). Requirement 6 (R6) defines the integration in existing systems and processes of the command and control center systems in detail, including the specific consensus mechanisms for sending and answering a dispatch request (R6.1), for requesting and delivering operating resources (R6.2), for automated and manual sending of geospatial information objects (R6.3), for confirmation of received messages (R6.4), for sending a read receipt (R6.5), and for active information regarding information receipt (R6.6). Goals and requirements were used to develop the artifact iteratively, which is described in detail in the next section. The framework was evaluated based on an evaluation scheme [32] and use cases. More details regarding the evaluation are described in Section 4.2, "Evaluation."

# 4. Framework

The result of the structured DSR process is a framework for the application of blockchain technology in emergency response derived from the stated goals and requirements. The achievement of the goals and fulfillment of the requirements are documented within the description of the framework. Furthermore, the findings of the evaluation of the artifact are described again according to the stated goals and requirements.

## 4.1 Framework description

The proposed framework connects existing command and control centers (C2s). C2s usually operate an application architecture (application servers and mechanisms), databases, and a user interface to interact. The C2s (nodes) use a defined communication interface to interact using

blockchains, which means achieving goals G4 and G5 with respect to efficiency. Resulting from the nature of the blockchain technology, this basic design even fulfills requirements R1, R3, and R6, [10]. Requirement R1.1 for identity and access management can be met by the application of asynchronous encryption [11] or by a specific governance (set up by the operator), in this case of a private blockchain [46]. The encryption method (e.g., using a public key [11]) can also be used to identify and address the node (R2.1). Scalability and transaction speed (R1.2 and R1.3) are interdependent. The number of transactions is limited by the size of the block, and a new block can only be added after the validity is granted by another node [39, 50]. Thus, scalability is limited by the number of transactions (number of blocks) and the associated validation process. According to R1.2 and R1.3, this must be harmonized with the number of accepted nodes [46] within one network. To fulfill requirement R2.2, the term information channel is used synonymously with the term blockchain, as every blockchain is interpreted as an information channel with a certain task. In this case, these channels are "Inform & Record," "Incident Resources," and "Geo-Objects." Each blockchain must communicate with a non-blockchain architecture, in this case, the C2's communication interface (R1). Blockchain technologies can be both interoperable and intra-operable [46]. To meet the demand for high availability according to information interchange and storage (R3.1 and G5), the blockchain infrastructure must follow a non-monolithic design. In addition, the network infrastructure must be decentralized and independent from a common global network node list. As consensus mechanisms vary in (energy) efficiency [34] and catastrophic events often harm the energy supplying the infrastructure [5], simple yet useful mechanisms (e.g. "proof of authority" [51]), must be established. They allow blocks to be solely added by trustworthy C2s (G5 and R3.1). These nodes must be associated clearly to a certain entity in reality. This also supports requirement R3.2, especially because traceability and verifiability [51] are granted by consensus mechanisms. All transactions and events taking place among the nodes are saved within the distributed ledger [10]. Integrity is granted due to hash functions and the chaining of the blocks [39]. The requirement of transparency concerning the time sequence (R3.3) is also fulfilled, as the headers of the blocks show timestamps on all transactions [11]. Combined with the fact that blocks cannot be deleted, this leads to a gapless chronology of all events and transactions. The interchange of data on incident vehicles (R5) and geo-objects (geospatial objects; R4) in blockchain technology is doubtlessly applicable, as (R1) to (R3) are also granted, and is highly independent of the complexity of the exchanged data.

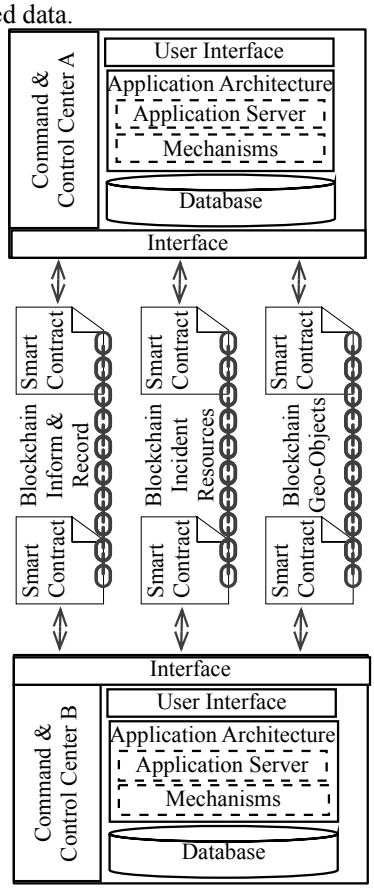


**Figure 2: Framework architecture**

Furthermore, attempts to normalize and standardize blockchain technology are being initiated [40]. Common formats for data exchange can manage geo-objects (e.g., OASIS EDXL, NATO JC3IEDM, and DIN SPEC 91287). The abstract geo-object can be associated with a broad spectrum of use cases. All participants must come to a mutual agreement on the syntax and semantics of the exchanged data, as this is crucial for message passing.

As our literature review shows, currently, no governmental approach exists to regulate individual-related data in the blockchain data structures (focus: Central Europe). Therefore, being compliant with the General Data Protection Regulations (e.g., deletion of data) and using blockchain technology is complicated to realize (R3.4). As all interviewees agreed that individual related data is not necessarily highly available, data exchange can be handled off-chain. The need for the handover of resources can be managed analogously to the transfer of property rights in the case of crypto currencies (e.g., using tokenizing). The ISSI can be managed as properties

and handed over with the use of tokens (R5). To meet R6, the applied framework must support smart contracts. Because Turing complete smart contracts can be run on the nodes [14], such contracts must be defined and implemented to allow communication via interfaces. To realize R6.4, R6.5, and R6.6, a specified blockchain must be established. This independent blockchain could also perform the key management for encryption (e.g., for resources or geo-objects) and record off-chain data interchange (R3.3). Figure 2 shows the design of the framework architecture, the C2, and the planned three-fold blockchain application for protocol and logging, resources, and geo-objects.

## 4.2 Evaluation

As shown above, the framework can meet the solution-neutral demands of the interviewed experts from a theory-based view.

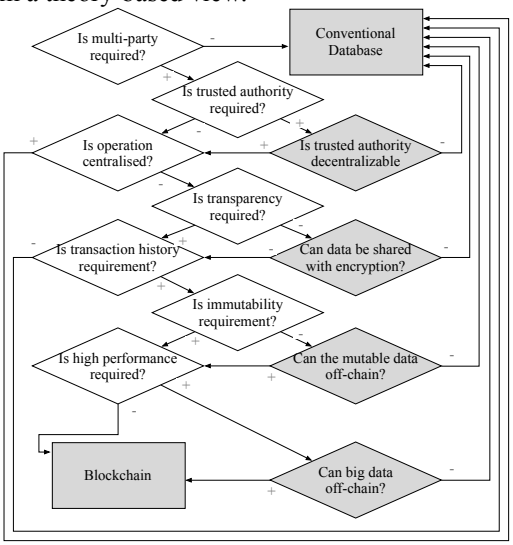


**Figure 3: Suitability evaluation framework [adopted from 32]**

According to [32], the evaluation of the applicability of blockchain technology for an application area is a complex task because of the lack of (product) data and uncertain (reliable) technology evaluation. They suggested using a "suitability evaluation framework" that evaluates the suitability/applicability of a use case according to its characteristics (attributes) and not because of a (technical) component description. The framework uses a decision tree structure (Figure 3).

Three fundamental use cases associated with the three blockchain applications were derived to completely describe all characteristics. Figure 4 shows the use case dealing with (regular) dispatching and alerting.

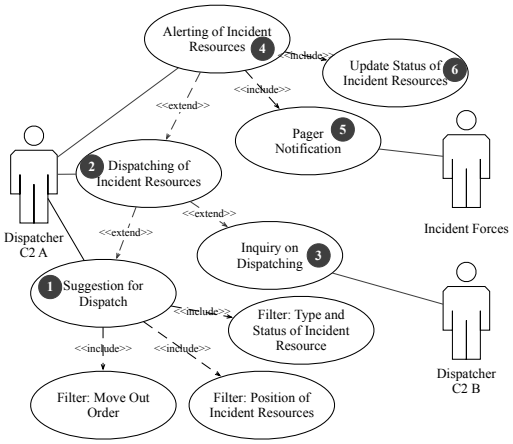


**Figure 4: UC 1 (dispatching and alerting)**

The numbers indicate a common sequence in the case. After an emergency is registered, the controller of C2 A receives a suggestion (1) for the dispatching based on the current move-out order, the current position and type, and the availability (status) of incident resources, as saved in the blockchain (incident resources and geo-objects). If the dispatcher accepts the suggestion, incident resources are alerted (4), and in the case of external operation resources, they are requested from the responsible C2 (3). Requests and decisions are stored in the blockchain ("Inform & Record"). If the request is granted by controller C2 B, the incident resource can be dispatched (2). The ISSI (received from the blockchain) is used to alert the incident forces (5). The new status of the forces is updated and stored in the blockchain (incident resources), and the whole process is logged ("Inform & Record").

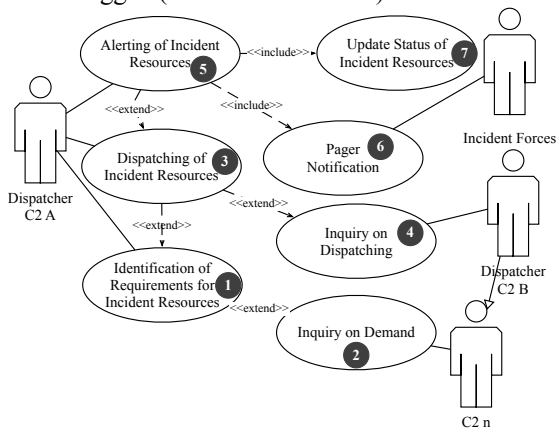


**Figure 5: UC 2 (incident resource demand)**

The second use case is displayed in Figure 5. It is initiated by registering the demand for a group of incident resources (supra-regional demand).

After the demand is registered, an identification of the requirements associated with geospatial information is initiated (1). The demand and process

are logged in blockchain ("Inform & Record"). If the demand can be met (2), an offering is sent to C2 A. The dispatcher now can accept the offering (3). In this case, another inquiry is sent to controller C2 B to address rapidly changing emergency scenarios (4, stored in blockchain "Inform & Record"). Then, incident resources can be alerted (5) and the process is the same as in the use case (dispatching and alerting).

The third use case deals with the collection and management of geospatial data.

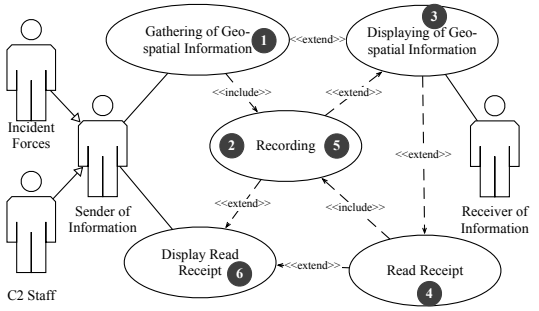


**Figure 6: UC 3 (geospatial data)**

(1) After geo-information is registered, it is stored in the blockchain (geo-objects). The request is registered (2) in the blockchain ("Inform & Record"), and the smart contract informs the recipients of the information. If the recipient is validated, the information is displayed (3), and a read receipt is generated (4). Smart contracts inform the dispatcher of the read receipt and store the transaction (5). Finally, the read receipt is displayed (6).

**Table 2: Results from the evaluation**

| Question/Use Case | 1 | 2 | 3 |
|---|---|---|---|
| Is multi-party required? | 1 | 1 | 1 |
| Is trusted authority required? | 0 | 0 | 0 |
| Is trusted authority decentralizable? | - | - | - |
| Is operation centralized? | 0 | 0 | 0 |
| Is transparency required? | X | X | X |
| Can data be shared with encryption? | 1 | 1 | 1 |
| Is transaction history required? | 1 | 1 | 1 |
| Is immutability required? | 1 | 1 | X |
| Can the mutual data off-chain? | - | - | 1 |
| Is high performance required? | 1 | 1 | 1 |
| Can big data off-chain? | 1 | 1 | 1 |
| Result (suitable) | 1 | 1 | 1 |

The application of the three use cases on the suitability evaluation framework led to the results shown in Table 2 (Legend: "1": yes; "0": no; "X": partially; "-": transitive). Following the evaluation scheme by [32], the defined use cases are suitable to be implemented with blockchain technology.

## 5. Discussion

As mentioned above, the aim of this study is designing and evaluating a framework for the adoption of blockchain technology in the case of emergency response. Based on various sources (academic literature, applicable laws and regulations, and interviews with experts), we developed and evaluated the framework by applying a DSR approach. Therefore, our artifact and the related knowledge gained from the study contribute to research and real-world applications alike. On one hand, we showed how blockchain technology seems to meet all the desired requirements for trust and information security. Since the blockchain can be individually configured, it can be specifically designed to meet the requirements for an information channel between participants. As a result, entire architectures with multiple blockchains ("Inform & Record," "Incident Resources," and "Geo-Objects") are solutions to interconnect multiple command and control center systems and mobile emergency units. Because of the needed availability in emergency scenarios, distributed and efficient blockchain layouts are more suitable than monolithic and resource-intensive layouts. In particular, the need for timely, accurate, and reliable information [7, 27] seems to be met by blockchain technology. Interestingly, our study revealed that the goals and requirements of emergency response resemble key concepts of information security management. For example, confidentiality, integrity, and availability [44] play an important role [1, 52], even non-repudiation, authentication, and authorization are directly related to the stated goals and requirements (e.g., G5.2, R3, and R4). General characteristics of information technology (IT) networks like scalability and the speed of transactions were addressed by the interviewees and were formulated as requirements for emergency response (e.g., R1.1 and R1.2), to give some examples. We assume that this is a valid starting point for further research in this area, in particular regarding the key concepts of information security and the application of blockchain technology in specific context environments.

In general, the practicability of the framework should be investigated in a broader manner. The empirically derived requirements are not only valid for fire departments, as most interviewees agreed in principle. Still, additional requirements could result from certain demands of police, rescue or even military services. The more organizations are involved, complexity increases and the more identity management and trust becomes relevant. The use of the blockchain for supporting identity management

[15, 54] and discussions on trust [4, 26] can serve as a starting point to analyze the potential in cases of emergency incidents or natural disasters in an overall setting. Regarding the practical application of the framework, we are currently discussing the implementation of the technology with the case fire department. It is planned to implement a proof of concept with partners from industry to show the applicability of the blockchain technology in this context.

## 6. References


[1] Adler, C., M. Krüsmann, T. Greiner-Mai, A. Donner, J.M. Chaves, and À.V. Estrem, "IT-Supported Management of Mass Casualty Incidents: The e-Triage Project", Proceedings of the 8th International ISCRAM Conference, (2011), 1–5.

[2] Allen, D.K., S. Karanasios, and A. Norman, "Information sharing and interoperability: the case of major incident management", European Journal of Information Systems 23(4), 2014, pp. 418–432.

[3] Arnott, D., and G. Pervan, "Design Science in Decision Support Systems Research: An Assessment using the Hevner, March, Park, and Ram Guidelines", Journal of the Association for Information Systems 13(11), 2011, pp. 923–949.

[4] Auinger, A., and R. Riedl, "Blockchain and Trust: Refuting Some Widely-held Misconceptions", Proceedings of the International Conference on Information Systems - Bridging the Internet of People, Data, and Things, ICIS 2018, San Francisco, CA, USA, December 13-16, 2018, (2018).

[5] Baldini, G., S. Karanasios, D. Allen, and F. Vergari, "Survey of Wireless Communication Technologies for Public Safety", IEEE Communications Surveys & Tutorials 16(2), 2014, pp. 619–641.

[6] Beck, R., M. Avital, M. Rossi, and J.B. Thatcher, "Blockchain Technology in Business and Information Systems Research", Business & Information Systems Engineering 59(6), 2017, pp. 381–384.

[7] Bharosa, N., J. Lee, M. Janssen, and H.R. Rao, "A case study of information flows in multi-agency emergency response exercises", Digital Government Society of North America (2009), 277–282.

[8] Bodenbenner, P., S. Feuerriegel, and D. Neumann, "Design Science in Practice: Designing an Electricity Demand Response System", In J. vom Brocke, R. Hekkala, S. Ram and M. Rossi, eds., Design Science at the Intersection of Physical and Virtual Design. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, 293–307.

[9] Cai, G., "Extending Distributed GIS to Support Geo-Collaborative Crisis Management", Annals of GIS 11(1), 2005, pp. 4–14.

[10] Chatterjee, R., and R. Chatterjee, "An Overview of the Emerging Technology: Blockchain", 2017 3rd International Conference on Computational Intelligence and Networks (CINE), IEEE (2017), 126–127.

[11] Christidis, K., and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", IEEE Access 4, 2016, pp. 2292–2303.

[12] Crosby, M., Nachiappan, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman, "BlockChain Technology: Beyond Bitcoin", Applied Innovation Review (2), 2016, pp. 16.

[13] Davidson, S., P. De Filippi, and J. Potts, "Economics of Blockchain", SSRN Electronic Journal, 2016.

[14] Dinh, T.T.A., R. Liu, M. Zhang, G. Chen, B.C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems", IEEE Transactions on Knowledge and Data Engineering 30(7), 2018, pp. 1366–1385.

[15] Dunphy, P., and F.A.P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain", IEEE Security & Privacy 16(4), 2018, pp. 20–29.

[16] Fill, H.-G., and F. Härer, "Knowledge Blockchains: Applying Blockchain Technologies to Enterprise Modeling", 51st Hawaii International Conference on System Sciences, HICSS 2018, Hilton Waikoloa Village, Hawaii, USA, January 3-6, 2018, (2018), 1–10.

[17] Gilbert, S., and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services", ACM SIGACT News 33(2), 2002, pp. 51.

[18] Gregor, S., and A.R. Hevner, "Positioning and Presenting Design Science Research for Maximum Impact", MIS Quarterly 37(2), 2013, pp. 337-A6.

[19] Herlihy, M., "Blockchains from a distributed computing perspective", Communications of the ACM 62(2), 2019, pp. 78–85.

[20] Hevner, A.R., "A three cycle view of design science research", Scandinavian Journal of Information Systems 19(2), 2007, pp. 4.

[21] Hevner, A.R., S.T. March, J. Park, and S. Ram, "Design Science in Information Systems Research", Management Information Systems Quarterly No. 1(Vol. 28), 2004, pp. 75–105.

[22] Hyvärinen, H., M. Risius, and G. Friis, "A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services", Business & Information Systems Engineering 59(6), 2017, pp. 441–456.

[23] Kane, E., "Is Blockchain a General Purpose Technology?", SSRN Electronic Journal, 2017.

[24] Kapsammer, E., B. Pröll, W. Retschitzegger, W. Schwinger, M. Weißenbek, and J. Schönböck, "The Blockchain Muddle: A Bird's-Eye View on Blockchain Surveys", Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services - iiWAS2018, ACM Press (2018), 370–374.

[25] Karahannas, M., and M. Jones, "Interorganizational Systems and Trust in Strategic Alliances", ICIS Proceedings 1999, (1999), 13.

[26] Khalifa, D., N.A. Madjid, and D. Svetinovic, "Trust Requirements in Blockchain Systems: A Preliminary Study", 2019 Sixth International Conference on Software Defined Systems (SDS), IEEE (2019), 310–313.

[27] Killeen, J.P., T.C. Chan, C. Buono, W.G. Griswold, and L.A. Lenert, "A Wireless First Responder Handheld Device for Rapid Triage, Patient Assessment and Documentation during Mass Casualty Incidents", AMIA 2006 Symposium Proceedings, (2006), 429–433.

[28] Kraut, R.E., D. Gergle, and S.R. Fussell, "The Use of Visual Information in Shared Visual Spaces: Informing the Development of Virtual Co-Presence", CSCW '02 Proceedings of the 2002 ACM conference on Computer supported cooperative work, ACM (2002), 31–40.
[29] Kuehn, A., M. Kaschewsky, A. Kappeler, A. Spichiger, and R. Riedl, "Interoperability and Information Brokers in Public Safety: An Approach toward Seamless Emergency Communications", Journal of theoretical and applied electronic commerce research 6(1), 2011, pp. 43–60.
[30] Ley, B., V. Pipek, C. Reuter, and T. Wiedenhoefer, "Supporting improvisation work in inter-organizational crisis management", Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12, ACM Press (2012), 1529.
[31] Lindman, J., V.K. Tuunainen, and M. Rossi, "Opportunities and Risks of Blockchain Technologies: A Research Agenda", (2017).
[32] Lo, S.K., X. Xu, Y.K. Chiam, and Q. Lu, "Evaluating Suitability of Applying Blockchain", 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), IEEE (2017), 158–161.
[33] Mao, M., and H. Xiao, "Blockchain-based Technology for Industrial Control System CyperSecurity", Proceedings of the 2018 International Conference on Network, Communication, Computer Engineering (NCCE 2018), Atlantis Press (2018).
[34] Mattila, J., "The Blockchain Phenomenon - The Disruptive Potential of Distributed Consens Architectures.", ETLA Working Papers No. 38, 2016.
[35] Meissner, A., T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, "Design Challenges for an Integrated Disaster Management Communication and Information System", The First IEEE Workshop on Disaster Recovery Networks, (2002).
[36] Meum, T., and B.E. Munkvold, "Information Infrastructure for Crisis Response Coordination: A Study of Local Emergency Management in Norwegian Municipalities", Proceedings of the 10th International ISCRAM Conference, (2013), 84–88.
[37] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf,
[38] Nilsson, E.G., and K. Stølen, "Ad Hoc Networks and Mobile Devices in Emergency Response – A Perfect Match?", In J. Zheng, D. Simplot-Ryl and V.C.M. Leung, eds., Ad Hoc Networks. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, 17–33.
[39] Nofer, M., P. Gomber, O. Hinz, and D. Schiereck, "Blockchain", Business & Information Systems Engineering 59(3), 2017, pp. 183–187.
[40] Pappert, T., F. Brauner, O.A. Mudimu, A. Lechleuthner, and A. Lotter, "IT-gestütztes Informationsmanagement in grenzüberschreitenden G roßschadensereignissen", pp. 11.
[41] Peffers, K., T. Tuunanen, M.A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research", Journal of Management Information Systems 24(3), 2007, pp. 45–77.
[42] Reuter, C., T. Ludwig, and V. Pipek, "Ad Hoc Participation in Situation Assessment: Supporting Mobile Collaboration in Emergencies", ACM Transactions on Computer-Human Interaction Vol. 21, No. 5, Article 26, 2014, pp. 26:1-26:26.
[43] Riedl, R., A. Benlian, T. Hess, D. Stelzer, and H. Sikora, "On the Relationship Between Information Management and Digitalization", Business & Information Systems Engineering 59(6), 2017, pp. 475–482.
[44] Samonas, S., and D. Coss, "The CIA strikes back: Redefining Confidelity, Integrity and Availability in Security.", Journal of Information System Security 10(3), 2014.
[45] Strauss, A., and J.M. Corbin, Basics of qualitative research: Grounded theory procedures and techniques., Sage Publications, Inc, 1990.
[46] Tasca, P., and C.J. Tessone, "Taxonomy of Blockchain Technologies. Principles of Identification and Classification", 2018, pp. 43.
[47] Tatham, P., and G. Kovács, "Developing and Maintaining Trust in Hastily Formed Relief Networks", In Relief Supply Chain Management for Disasters: Humanitarian Aid and Emergency Logistics. IGI Global, Hershey, 173–195.
[48] Törnqvist, E., "Hastily Formed Networks for Disaster Response: Technical Heterogeneity and Virtual Pockets of Local Order", 2009, pp. 5.
[49] Williams, A.P., "Agility and Interoperability for 21st Century Command and Control", The International C2 Journal Vol. 4, No. 1, 2010, pp. 32.
[50] Xu, X., C. Pautasso, L. Zhu, et al., "The Blockchain as a Software Connector", 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), IEEE (2016), 182–191.
[51] Yaga, D., P. Mell, N. Roby, and K. Scarfone, Blockchain technology overview, National Institute of Standards and Technology, Gaithersburg, MD, 2018.
[52] Zambrano, M., F. Pérez, M. Esteve, and C. Palau, "Interoperability in the emergency management. A solution based on distributed databases and P2P networks", Computer Science and Information Systems 15(2), 2018, pp. 257–272.
[53] Zheng, Z., S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey", International Journal Web and Grid Services (Vol. 14, No. 4), 2018, pp. 352–375.
[54] Zhu, X., and Y. Badr, "A Survey on Blockchain-Based Identity Management Systems for the Internet of Things", 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE (2018), 1568–1573.
[55] Zlatanova, S., and A.G. Fabbri, "Geo-ICT for Risk and Disaster Management", In H.J. Scholten, R. van de Velde and N. van Manen, eds., Geospatial Technology and the Role of Location in Science. Springer Netherlands, Dordrecht, 2009, 239–266.