Enhancing the security and transparency of critical reporting and process chains with blockchains

FUJITSU | HEXAGON

Contents

Introduction

What are critical reporting chains and why are they important? – A brief summary

A functioning energy, water and food supply, an efficient transport system and a working healthcare or telecommunications system are vital to modern society. Malfunctions, failures, accidents in these areas can have negative financial, economic and sometimes even macroeconomic consequences (and therefore being more often targeted by malicious actors). They can impact people's trust in the government, authorities and individual companies, especially if the responsible parties blame each other after an incident. In modern and complex infrastructures, numerous processes define how different parties interact in certain situations. The input for these processes and interactions is provided by humans and, in an increasingly digital world, by sensors embedded in all kinds of devices. Within large process environments, some processes define how parties must interact with each other in the case of incidents and emergencies. These processes are known as reporting chains.

A reporting chain is a sequence of action steps taken to handle incidents within a designated process environment. Each step is triggered by a specific event and initiates a specific action in response to this event. An action might be to transfer information to relevant stakeholders or to implement/initiate specific measures to address the situation at hand. Therefore, the goal of a reporting chain is to ensure that all relevant stakeholders follow a specific protocol to mitigate or prevent any negative effects resulting from an incident.

For example, an accident in a production facility would require the line manager/supervisor to evaluate the incident, call an ambulance, temporarily stop production, etc. Depending on the situation, the incident may have to be escalated to management and the production shutdown extended until enhanced security measures are in place.

If the reporting chain's underlying process is critical, i.e. if an improperly handled incident can cause serious or even catastrophic consequences beyond the ultimate process environment, this is known as a critical reporting chain. The proper transfer of information, the involvement of relevant stakeholders and the quick initiation of protective or preventive countermeasures are thus especially important and valuable for a critical reporting chain.

For example, a harmful substance leaking from an industrial plant into the environment can severely impact nature and human beings in the local area and even the wider region. Due to the possible magnitude of these effects, it is important that all parties involved in the critical reporting chain follow the protocol designed to handle such an event to contain the problem and mitigate potential harm to the surroundings.

Due to the sensitivity and the scope of the underlying processes, the stakeholder environment of a critical reporting chain often comprises numerous different parties who need to interact with each other.

This means that many stakeholders may exchange information, thus increasing the complexity of the critical reporting chains. This adds an additional layer of trust and dependency that needs to be accepted by all stakeholders, who must rely on the validity of the data they receive from other parties. Because a non-functioning critical reporting chain can have serious consequences, a supervisory authority audits the entire chain of events and actions should such a scenario arise. The parties found to be responsible for the failure as a result of the audit will face liability claims and litigation. To avoid these risks, it is crucial for any stakeholder of a critical reporting chain to be able to prove compliance with the protocol and to verify information received from other parties in the critical reporting chain. If the impact is catastrophic – such as that caused by a natural disaster – information floats around in multiple paths and is very hard to trace. For example, one year after the disastrous floods in the Ahrtal (Germany) in 2021, audit teams are still trying to reconstruct the flow of information and decisions taken during that event to assess the response to the disaster.

Multiple parties and multiple trust layers

When discussing the ongoing and upcoming activities of smart cities/regions and digital twins, one topic deserves to take center stage: trust. When stakeholders collaborate, depend on each other or make decisions in hybrid environments, trust is key.

Different levels of trust need to be considered:

- Between organizations
- Between departments within one organization
- On a technical level, for example between a sensor and the decision support system

Decision support systems as well as command & control systems rely on the correctness of the received data/information. Similarly, all activities in critical environments have to be documented in order to audit events, decisions and actions. An audit's complexity increases dramatically when multiple stakeholders are involved.

In a multi-party ecosystem, the auditing process can be a potential risk for the actors involved:

- Sensors can emit misleading data due to misconfiguration, malfunction, failure or manipulation from a malicious entity, leading to wrong decisions.
- Compliant actors need to provide proof during the audit to avoid being held liable for wrongdoing or negligence.
- Noncompliant actors are motivated to fabricate claims in order to avoid being held liable.
- Auditors are expected to extract the facts from potentially contradicting claims and data.

Blockchain technologies can support scenarios where the exchange of information must be secure and verifiable. Instead of relying on a single party to verify the data's status and the action history, blockchains use cryptography and special algorithms to reach consensus on such status at any given time. They do this in such a way that the data and actors involved are cryptographically verifiable and undeniable.

The initial and best-known use case is cryptocurrency, where users can exchange value in the form of cryptographic tokens, without relying on a bank for updating the balance-sheets after each transaction. As blockchain technologies have evolved, they are no longer limited to only providing a transparent and secure ledger. Indeed, they have become decentralized application execution environments. Blockchain technology can thus address scenarios beyond the transfer of tokens. Such applications first led to a rapid rise in decentralized finance (DeFi), where complex financial instruments are implemented in the form of blockchain applications, and later to other numerous domains. Today, blockchains can be useful whenever communication transparency, data integrity and auditability are at stake in multi-stakeholder environments.

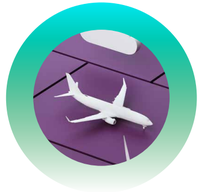
Based on these considerations, blockchain technology could also be valuable when handling critical alarms. It is essential to monitor sensors continuously.

One or multiple sensors can detect a situation, which might generate a digital alarm that triggers an action (e.g., fire yes/no). Alternatively, certain value trends may trigger the alarm (e.g., increasing temperature in a data center). Sensor technology is quite agile. Sensors with new, enhanced or combined technologies are being built and marketed in ever shorter cycles. Each new generation tends to become more intelligent, thus bringing a certain level of computing capacity to the device itself. Consequently, a sensor-agnostic environment is key to maintaining a resiliency that can benefit from the latest technologies.

Used between sensors and decision support systems, or between different stakeholders, blockchain technology provides the trust needed for transparency and indisputably tracking events, decisions and actions.

This white paper describes a critical reporting chain scenario based on a leading technology sensor with a blockchain client on board, an IoT platform and several participating stakeholders. This scenario demonstrates the value of a trusted sensor and a trusted partnership between the stakeholders. The paper then dives deeper into technical aspects of the sensor, the blockchain and the monitoring environment.

Examples of critical infrastructures

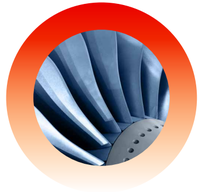


Transportation

Water systems

Telecommunications

Energy



Defense

Reference use case

Due to rapid climate change, phenomena linked to weather and climate extremes, such as heat waves, forest fires, heavy precipitation, flood events, storms and storm surges, happen more frequently and in areas where they never used to occur. These types of events can directly or indirectly cause major damage and impose a significant financial and economic burden on the affected regions, and they also have the potential to cost many human lives.

The management and handling of flood events is a highly critical and complex procedure that requires numerous organizations to work together. It is crucial to install a critical reporting chain (CRC) that includes processes and infrastructure specifically designed to handle such events to prevent or mitigate the probability of catastrophic outcomes. The impact of such events on society can be of such magnitude that additional mechanisms must be implemented to verify the functionality of the CRC and thereby strengthen public trust in these processes and the stakeholders involved. When it comes to handling flood events, a CRC, enriched by blockchain technology, can provide substantial value to society.

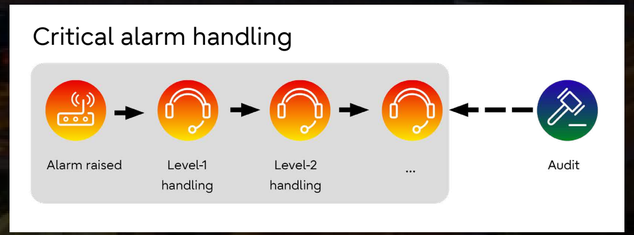
Reference use case

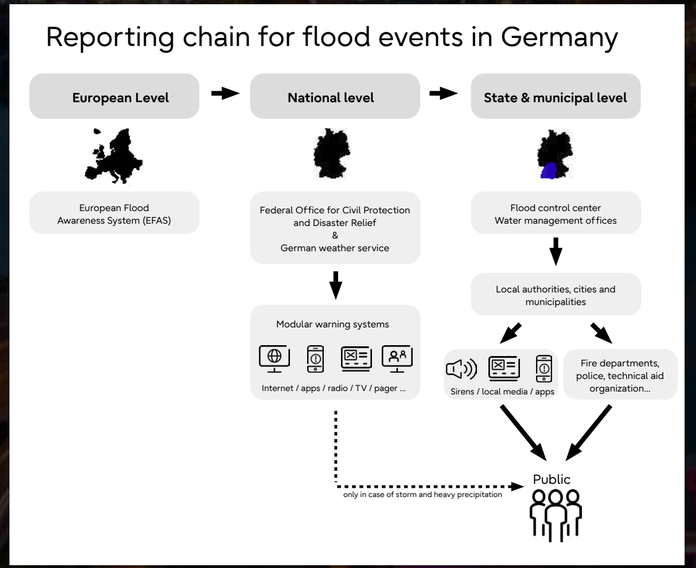
According to findings of the 2018 United States Geological Survey, floods account for more than 75 percent of federal natural disasters in the United States and are responsible for more than 90 fatalities as well as a financial damage of several billion dollars per year. However, the United States is not the only country experiencing greater flooding. Due to climate change and increased urbanization in flood-hazard areas, floods pose a threat to a growing number of people in many regions around the world, and the number of fatalities can easily run into the thousands.

The handling and management of flood events in Germany is a good example of a CRC. Multiple stakeholders need to communicate and coordinate with each other at different levels of authority, each with different areas of responsibility. The entire process involves multiple steps that must run smoothly to initiate the relevant measures in the flood-impacted regions and to mitigate the probability of negative outcomes. The following overview describes a general approach. Each German state has its own procedure for handling and managing floods.

The European Flood Awareness System (EFAS) is usually the first stakeholder to get involved in managing flood events. EFAS is a European Commission initiative that monitors and forecasts flooding across Europe and works as an early warning system. It provides probabilistic data and information about floods up to ten days in advance and thus aims to support preparations prior to major flood events. EFAS reports relevant information to other organizations, including those responsible for flood management at the national level. Note that EFAS is a data provider, and it may also issue recommendations for flood management. However, it lacks the authority to take action at the national or state level. In Germany, this information is provided to the Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) and Deutscher Wetterdienst (DWD). The DWD assesses the information it receives from EFAS and reports it to state authorities. If the data points to events such as storms or heavy precipitation, the DWD is authorized to alert the public. However, the DWD does not issue warnings regarding flood events, which may only be initiated at the state or municipal level. This mechanism is intended to prevent confusion resulting from multiple authorities distributing conflicting information about flood events to the public. Moreover, local authorities have a better overview of the local situation, which allows them to take proper action.

Once state authorities have received information about a possible flood event, they may activate a reporting chain at the state and municipal level. The state authorities first process the information they received from DWD, after which they report relevant data (e.g., water level, flood forecasting) to municipal and city authorities. These authorities then inform the public of flood events and security measures (e.g., evacuation) using local information channels. The local authorities simultaneously organize and control the deployment of emergency services, which help implement the security measures and keep the people safe.





The involvement of numerous stakeholders at different levels and across different jurisdictions creates a highly diverse ecosystem. Relevant data must be collected, processed and reported to many different recipients. This step is challenging because in this kind of a top-down setup, high-level authorities have the resources to conduct comprehensive data collection and processing. Local authorities, however, usually have limited resources to analyze and interpret data. Therefore, any data reported along the chain of authority must contain all relevant in-depth information in a format that allows the recipients to process the data quickly and easily. When it comes to flood prevention, time is also of the essence. Therefore, it is not only important to forward relevant and comprehensible information, but it is also crucial that decision-makers receive information as early as possible.

The heterogenous landscape of communication tools and reporting methods along the reporting chain presents another challenge. This heterogeneity is especially pronounced at the state and municipal levels, where there is often a blend of partly digitalized and analogous processes. A fax, which must be manually sent, is commonly the key to triggering crucial events that may determine the success or failure of flood handling measures. This blend of digital and analogous reporting formats not only makes the process execution inconsistent, but it also disrupts the information flow, makes operations inefficient and is prone to error.

Benefits of blockchains in CRCs

The previously mentioned challenges may cause the reporting chain to fail and also obscure the effectiveness and efficiency of the stakeholders involved. Blockchain technology can address these challenges and thus contribute to society in a meaningful and valuable way.

Benefits of blockchains in CRCs

At its core, blockchain technology creates an immutable set of data records of all interactions between all stakeholders. In the CRC scenario, the blockchain stores and manages an immutable record of all relevant information that was passed along the chain of authorities. Therefore, a blockchain can generate significant value for all parties involved as well as for the public when it comes to handling flood events.

Using blockchain technology, all stakeholders can rely on the fact that the data they receive from other stakeholders and used as input for their own actions is of high integrity and tamper-proof. This can boost a stakeholder's confidence when making decisions in critical situations when there is little time to assess information provided by another party. Stakeholders can thus justify their behavior/decisions based on information that is immutably stored in the blockchain.

Blockchain technology provides an audit trail whose information integrity is indisputable. Auditors can rely on the data's integrity during the audit to extract reliable information about "who, what and when." This makes it easier to reproduce stakeholder actions along the reporting chain and makes the overall process more transparent. Hence, blockchain is an enabler of public trust in the integrity of critical processes and the governmental bodies involved, and also allows stakeholders verify their actions toward auditors and the public.

Another benefit of a blockchain is that it allows pain points in the CRC to be identified. Since all stakeholder actions are immutably stored in the blockchain, an analysis of the underlying data can provide crucial insights as to critical procedures within the CRC that may cause the entire process to fail. Thus, blockchain can help identify pain points and justify adjustments to the underlying process.

Critical reporting chain from sensor to emergency service

How can blockchain technology enable parties to realize substantial efficiency gains regarding the underlying process?

- A key requirement for deploying a blockchain is the digitalization of processes or at least critical process steps. To some degree, all stakeholders must also use a uniform data format when they interact with each other. To achieve this, stakeholders must adjust their processes, which makes it possible to establish uniform data and communication standards and thus harmonize the process environment along the whole reporting chain. This can result in higher operational efficiency, and it mitigates the risk of information loss along the stakeholder chain.

- A harmonized process landscape makes it possible to automate standardized process steps. Process automation can be realized using specific blockchain features, such as smart contracts, and non-blockchain tools. As such, a blockchain may reduce infrastructure and administrative overhead that is needed when the process is executed manually. As a result, blockchains can deliver value in the form of accelerated process execution and increased operational process efficiency.

The benefits that can be capitalized using blockchain are very versatile. The blockchain can enhance public trust in CRCs and the parties involved. It can also drive the digitization of critical processes, which increases their operational effectiveness and efficiency. This is particularly important in critical situations such as handling flood events. In general, the blockchain is a technology that can be of great value to society in multiple dimensions.

Want to learn more?

Here are some interesting links:

Learn more about the Flood Inundation Mapping (FIM) Program

Read the article “Three reasons the world is seeing more record-breaking deluges and flash floods.“

Find out: “Are there more floods now than there used to be?”

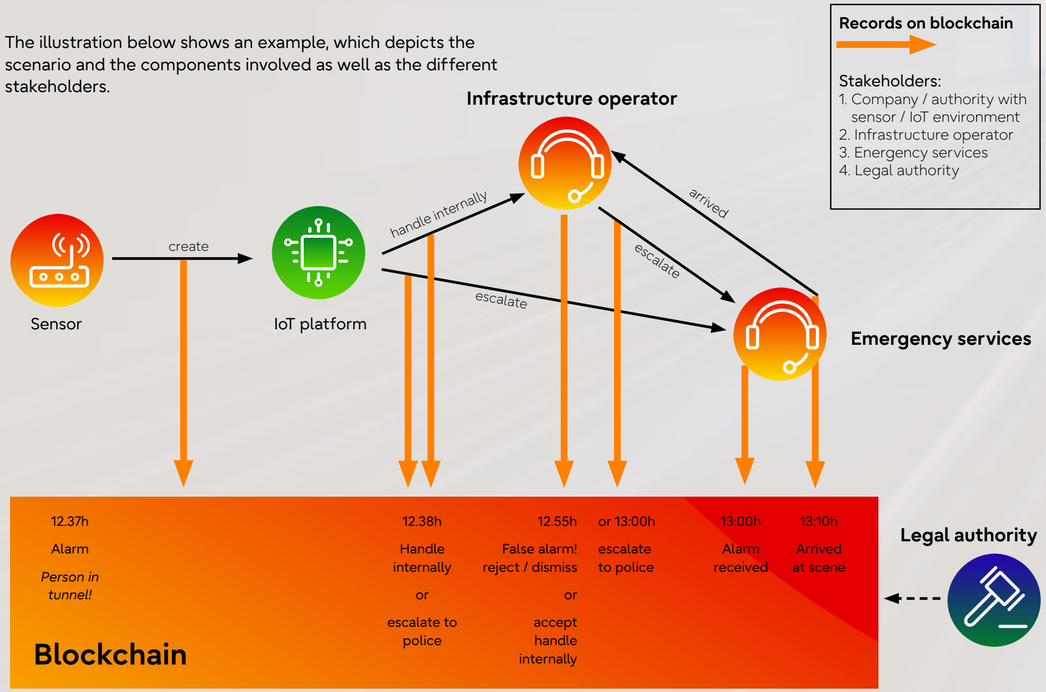
Watch our video: „Transparency, security and auditability of critical reporting chains with blockchain.”

Technology insights

In their joint efforts, Fujitsu and Hexagon use multiple technologies and platforms to implement blockchain technology in CRCs. In the following example, the solution consists of three core elements. It starts with a modern hybrid sensor that detects an event and triggers an alarm. The second component is the infrastructure, obtaining sensor feeds and enabling the operators to assess situations and take various counter-measures. The third element is the distributed ledger technology for permanently documenting information and creating a center of trust for all stakeholders.

The story at a glance

The illustration below shows an example, which depicts the scenario and the components involved as well as the different stakeholders.



BLK247 multi-sensor unit

The BLK247 from Hexagon Geosystems is a LiDAR-based (Light Detection and Ranging) security system that continuously monitors objects in 3D space. This sensor is a compact security device that consists of a LiDAR system and visual as well as thermal cameras. An on-board computational unit also executes different operations and serves as the hosting environment for the blockchain client.

The LiDAR system in the BLK247 allows the sensor to capture and record everything that happens around it in 3D, providing additional surveillance capabilities compared to pure 2D sensors. The BLK247 is also equipped with a 2D camera system that scans 360 degrees horizontally and 240 degrees vertically. The combination of 3D LiDAR and a 2D camera is interesting for GDPR. The 3D sensor monitors the environment continuously in full compliance with GDPR rules. Only if an alert is raised does the additional 2D sensor provide data to operators with video feeds (which otherwise can, in principle, raise GDPR issues). All sensors and alerts may potentially be linked to the blockchain. Depending on the use case, selective sensor states and sensor data are then documented.

The sensor's onboard automation system is extremely helpful in very busy environments where traditional security systems can struggle. And because the BLK247 uses LiDAR, this is all still possible in extremely low-light conditions and even in complete darkness. The existing capabilities make it possible to create virtual 3D zones that act as fences around particular areas (such as tunnel entries) or objects (such as ticket machines). The BLK247 can therefore monitor all activity automatically, even in very busy environments, and it can send an alert if something or someone crosses the established boundary.

As part of the project, the BLK247 was equipped with a software client as a direct interface with the distributed ledger technology to minimize the possibility of the surveillance system being compromised and to document the activities automated by the sensor (such as raising alarms).

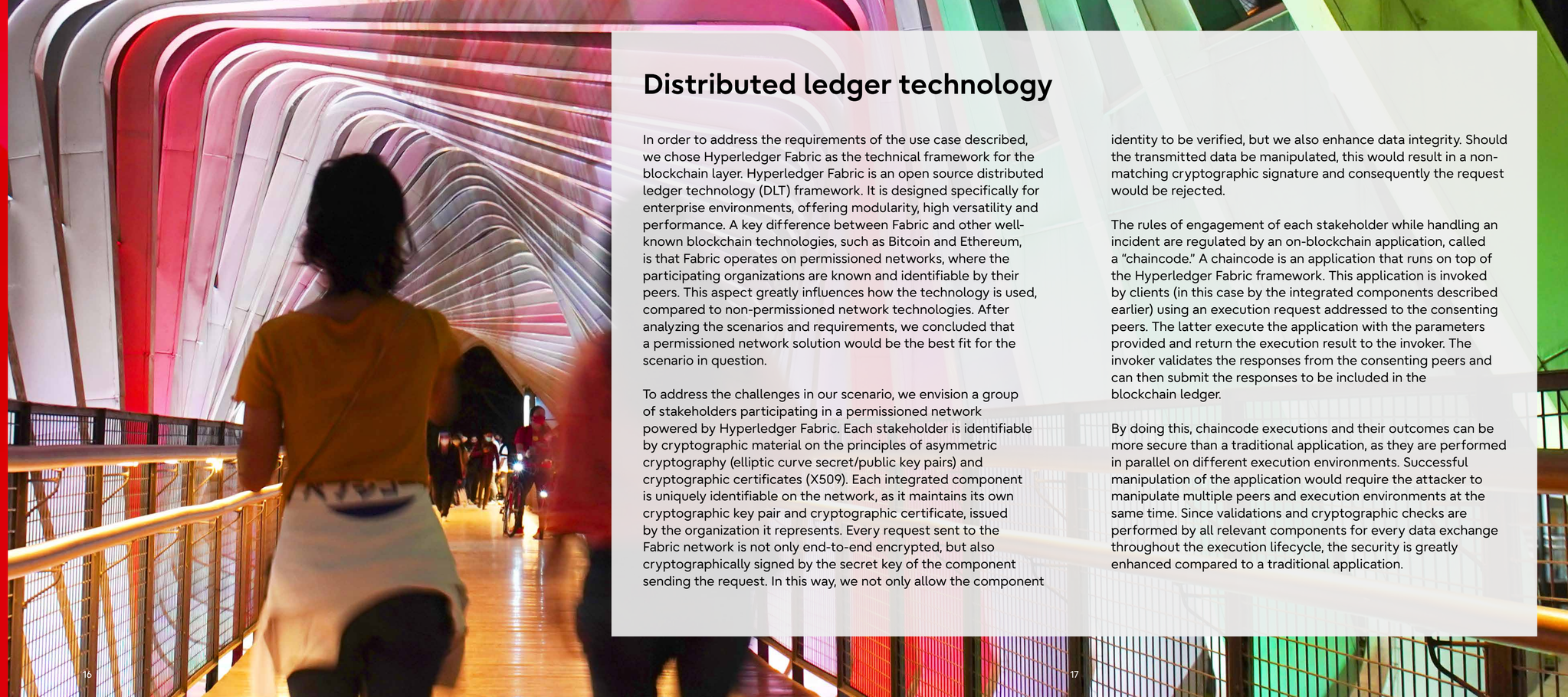
Value coming from the sensor BLK247

Awareness
The BLK247 provides true 3D values with image and temperature information to create situational awareness.

Reliability
True 3D change detection in space creates more reliable information to detect threats compared to 2D video devices.

Autonomy
On device threat detection uses assistive AI and edge computing to analyze the gathered data.

Sensor fusion
Situational awareness created with true 3D values, image and temperature information.



Distributed ledger technology

In order to address the requirements of the use case described, we chose Hyperledger Fabric as the technical framework for the blockchain layer. Hyperledger Fabric is an open source distributed ledger technology (DLT) framework. It is designed specifically for enterprise environments, offering modularity, high versatility and performance. A key difference between Fabric and other well-known blockchain technologies, such as Bitcoin and Ethereum, is that Fabric operates on permissioned networks, where the participating organizations are known and identifiable by their peers. This aspect greatly influences how the technology is used, compared to non-permissioned network technologies. After analyzing the scenarios and requirements, we concluded that a permissioned network solution would be the best fit for the scenario in question.

To address the challenges in our scenario, we envision a group of stakeholders participating in a permissioned network powered by Hyperledger Fabric. Each stakeholder is identifiable by cryptographic material on the principles of asymmetric cryptography (elliptic curve secret/public key pairs) and cryptographic certificates (X509). Each integrated component is uniquely identifiable on the network, as it maintains its own cryptographic key pair and cryptographic certificate, issued by the organization it represents. Every request sent to the Fabric network is not only end-to-end encrypted, but also cryptographically signed by the secret key of the component sending the request. In this way, we not only allow the component identity to be verified, but we also enhance data integrity. Should the transmitted data be manipulated, this would result in a non-matching cryptographic signature and consequently the request would be rejected.

The rules of engagement of each stakeholder while handling an incident are regulated by an on-blockchain application, called a “chaincode.” A chaincode is an application that runs on top of the Hyperledger Fabric framework. This application is invoked by clients (in this case by the integrated components described earlier) using an execution request addressed to the consenting peers. The latter execute the application with the parameters provided and return the execution result to the invoker. The invoker validates the responses from the consenting peers and can then submit the responses to be included in the blockchain ledger.

By doing this, chaincode executions and their outcomes can be more secure than a traditional application, as they are performed in parallel on different execution environments. Successful manipulation of the application would require the attacker to manipulate multiple peers and execution environments at the same time. Since validations and cryptographic checks are performed by all relevant components for every data exchange throughout the execution lifecycle, the security is greatly enhanced compared to a traditional application.

In the context of our project, the chaincode regulates the circumstances under which an actor is expected to take action and in which form. This is done throughout the complete handling process, from the moment an alarm is created.

All the critical information and the actor involved are recorded on the ledger. Finally, as the complete critical reporting chain and the relevant data is recorded on the ledger, the audit can be performed based on the data recorded, secured and timestamped on the blockchain, in a non-disputable manner.

When an IoT device transmits data, it typically communicates this information to an integration platform. In our approach, we introduce an additional communication channel for devices integrated into Hyperledger Fabric: An application deployed on the device transmits the alarm data to the Hyperledger Fabric network. During this process, the device is identified, the data is time-stamped and appended to the ledger of the peers in the network.

Data transmission is encrypted and signed with cryptographic material on the device, unique to each device. Each monitoring device thus has its own unique digital identity over the entire network. The next component integrated with Hyperledger Fabric is the IoT platform.

By being integrated with Hyperledger Fabric, this platform can intercept sensor data via two communication channels in parallel:

- "Traditional" direct communication with the device, via the APIs made available by the IoT Platform
- Novel communication via the Hyperledger Fabric platform

This enhances communication resiliency through redundancy. Moreover, the IoT platform is enabled to compare data received through its "traditional" APIs, with the data communicated via Hyperledger Fabric, and to verify the data integrity and the identity of the sensor. If the data comes from a device that cannot be integrated into Fabric directly, the IoT Platform can serve as a "trust anchor" for the IoT device. This means that the IoT platform can onboard the sensor data to Fabric on behalf of such sensors.

When the IoT Platform intercepts data, it may perform certain automated actions, depending on the IoT platform's configuration. For example, if the data values are recognized as "critical" due a threshold value, the IoT platform can take over and directly "escalate" the incident to the relevant stakeholder. Examples include data from fire detectors that automatically involve the fire department. Alternatively, the IoT platform may be expected to enhance the context of the situation by providing data from additional devices. In any case, the actions of the IoT platform are recorded on the Fabric peers and linked to its cryptographic identity.

To enable human operators to interact with Hyperledger Fabric, we have integrated the decision support systems/command & control systems. For this purpose, we provided an integration service with a dedicated API accessible to these systems. Each organization that is expected to intercept and react to events controls an instance of this integration service. The latter also maintains a cryptographic key pair and a cryptographic certificate, controlled by the host organization. This cryptographic material is used to interact with Hyperledger Fabric. The context, decisions and actions of the operators are recorded in the ledger. The relevant data is linked to the identity of the component and the host organization.

The final role to be integrated is the auditing organization. In order to enhance the audit process with the benefits of Hyperledger Fabric, we have provided a dashboard where incidents can be filtered by various attributes (e.g., time stamps, locality or by sensor identity). Through these dashboards, the data is retrieved directly via the DLT platform (distributed ledger technology, in this case Hyperledger Fabric). All the relevant information becomes available to the auditor with a few clicks. The event data, context and decisions of each involved party are easily accessible in a cryptographically verifiable and indisputable way.

Value coming from the blockchain

Risk reduction
Fraud, cyber crime, (data) manipulation

Time saving
Reduction of effort and transaction times

Cost saving
Reduction of costs, expensive intermediaires and middlemen

Creating trust
Transparent, shared use of processes, data and records

Smart monitoring ecosystem

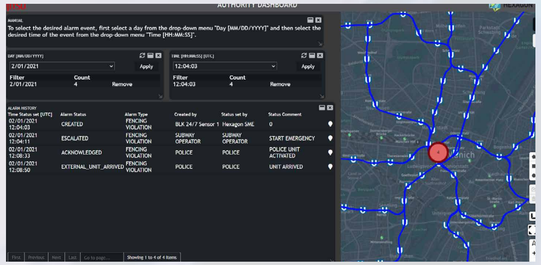
With massive amounts of location data being generated every minute, it can be difficult to not only determine what is operationally relevant, but also to access that relevant data as soon as it is produced to analyze it and act on it. One source of data to be considered here relates to the “Internet of Things” (IoT). IoT covers all sensors, from coffee maker switches to highly complex satellite sensors. In working with sensors, the key is to understand the capabilities and why they matter in a concrete solution needed to initiate activities. This directly relates to sensors like the BLK247 introduced earlier in this whitepaper.

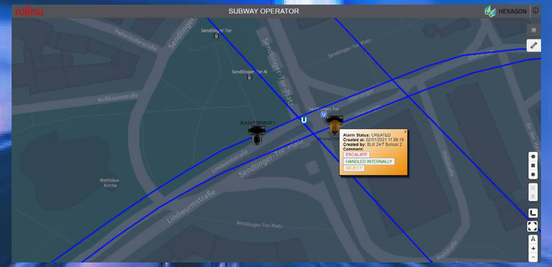
The smart monitoring ecosystem closes the gap by providing the framework for users to monitor and analyze IoT sensor data, as well as compare it to historical data, for both real-time analytics and trends analysis – even in 3D. Enhanced with deep learning and other machine learning capabilities, the smart monitoring ecosystem lets users focus on and keep track of how the assets they manage move and change, with the ability to automatically detect those changes. When specific occurrences affect an asset, notifications or alerts can be received through various channels to keep managers informed. Smart monitoring ecosystem for IoT also offers unlimited integration options for various sensor and data types without significant hardware or software requirements.

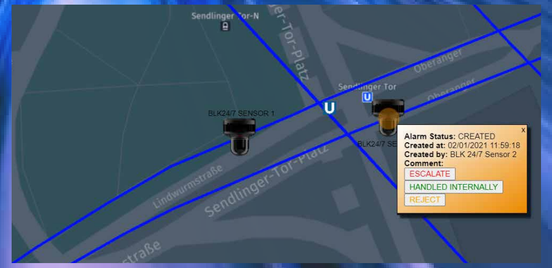
The ecosystem is a multi-tenant system, allowing different stakeholders to work on different or even the same instance.

Regardless of how the ecosystem is instantiated, the ability to read to and write from the distributed ledger technology is advantageous. First of all, the reading part is important, as it enables the system to validate the data received by the BLK247. Validation here means checking the correctness of the received events/alarms in detail. The writing part is equally important, as all decision and actions initiated through the use of the smart monitoring ecosystem were protocolled in the distributed ledger technology.

In this approach, the chain of parallel actions of multiple stakeholders and multiple users is seamlessly documented and can be repeated by authorized instances if an audit is needed.



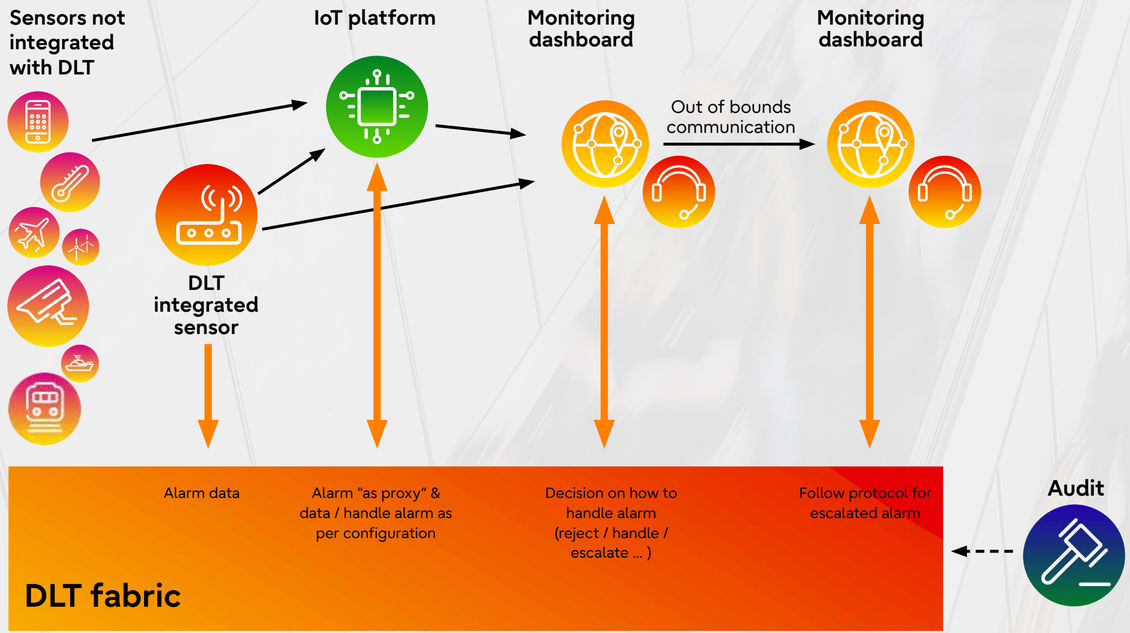




Value coming from the smart monitoring environment

- Establish reliable, real-time sensor connection
- Agile exploration process for dashboard configuration and exploitation of data
- Location intelligence by providing the relevant information
- Connect alarms, reporting chain and the blockchain

The DLT scenario at a glance



Conclusion and key facts

Conflicting claims that could lead to disputes are eliminated by using blockchain technologies. The information generated throughout the lifecycle of an alarm-handling process is recorded and accessible in a cryptographically verifiable and indisputable manner. The rules of engagement are defined in an application running on the blockchain platform in a way that cannot be bypassed regardless of the cause (e.g., human error or malicious actor). This eliminates friction and disputes when auditing events. The ease of performing an audit can allow security protocols to be optimized continuously and thus reduce risk during relevant events. Moreover, as all integrated components and stakeholders are uniquely identifiable on the network, very complicated ecosystems can be addressed, and information can be filtered automatically based on well-regarded systems that are completely transparent and indisputable. For example, sensors that are prone to communicate “false-positive” alarms can be identified and handled accordingly. The resulting data security, integrity and transparency can help enhance the public trust in how critical events are managed.

About the authors

Uwe Jasnoch, EMEA Director Government, Transportation and Defense at Hexagon

Uwe is an experienced leader with a proven history of increasing the performance of sales and technological organizations in the computer software industry. He has strong consulting skills in GIS, requirements analysis, computer science, AI & ML, enterprise software, agile methodologies, and databases.

Nikolaos Saklampanakis, Technical Lead for DLT/Blockchain at Fujitsu, Subject Matter Expert for Data & Security, and regional Fujitsu Distinguished Engineer

Nikolaos has a long technical background in multiple domains of the IT industry. He has covered roles such as technical consultant, software engineer, software and solution architect, as well as team lead and technical lead. He has lead teams that deliver innovative projects, while being in both start-ups and larger corporations.

He has been working with Blockchain technologies since 2016, in various projects for customers in both private and public sector. In December 2019, he joined Fujitsu as Technical Lead for DLT/Blockchain. His aim: To bring state-of-the art technologies together and drive innovation.

FUJITSU

Contact
00800 37210000
cic@ts.fujitsu.com
http://www.fujitsu.com

FUJITSU-PUBLIC
© Fujitsu 2023. All rights reserved. Fujitsu and Fujitsu logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.