UNIVERSITY OF TARTU
Institute of Computer Science
Innovation and Technology Management Curriculum

Svitlana Filipova

Modeling Business Processes on a Blockchain Ecosystem using CMMN

Master's Thesis (20 ECTS)

Supervisor(s): Fredrik Milani
Luciano García-Bañuelos

Tartu 2019

Modeling Business Processes on a Blockchain Ecosystem using CMMN

Abstract:

Blockchain has been speculated to be “the most important invention since the Internet” and has the potential to deliver significant business value for both financial and non-financial industries. That is why companies have started to explore how their business processes can benefit from this technology. However, a simple substitution of a current process with new technology will not provide desired outcomes. For this purpose, process redesign is used where process models are made the basis of process analysis and its innovation. This paper examines how blockchain-oriented processes can be modelled with CMMN as it is an artefact-centric modelling language. Such an approach might be particularly useful while modeling blockchain-oriented processes as the fundamental focus of blockchain is on data that is added on a chain and shared between participants. This paper is based on a case study of a non-profit organization providing certification services for companies trading timber-relates products. The auditing process of this organization was redesign using blockchain and smart contract technologies and then was modelled with CMMN. For analysis of the suitability of CMMN for modelling blockchain-based processes a framework for commonly occurring patterns that are specific to blockchain-based applications was used. As a result, CMMN can adequately represent blockchain-oriented processes. However, there is a lack of elements in the notation to accurately model certain details specific to blockchain and smart contract technologies.

Keywords:

Blockchain, CMMN, Business Process Models

CERCS: P170 Computer science, numerical analysis, systems, control

Äriprotsesside modelleerimine plokiahela ökosüsteemis CMMN-iga

Lühikokkuvõte:

Plokiahela kohta on spekuleeritud, et see on “kõige olulisem leiutis pärast Internetti” ning et sellel on potentsiaal pakkuda märkmisväärset ärilist väärtust nii finants- kui ka teistes sektorites. Sellest tulenevalt on ettevõtted hakanud uurima, kuidas oleks neil võimalik oma äriprotsessides plokiahelatehnoloogiast kasu saada. Siiski, lihtsalt olemasolevate protsesside asendamine uute tehnoloogiatega ei paku soovitud tulemusi. Sellest tulenevalt disainitakse olukordades, kus protsessimudelid on protsessianalüüsi ning selle innovatsiooni aluseks, protsesse täiesti ümber. Käesolevas töös uuritakse, kuidas plokiahelale orienteeritud protsesse saab modelleerida CMMN modelleerimiskeele abil, kuna see on artefakti-põhine modellerimiskeel. Selline lähenemine võib olla eriti kasulik plokiahelale orienteeritud protsesside modelleerimisel, kuna plokiahelate peamine fookus on andmetel, mis on lisatud ahelasse ning jagatud erinevate osapoolte vahel. Käesolev töö põhineb juhtumianalüüsil, mis on läbi viidud mittetulundusühingus, mis tegeleb puidutoodetega kauplevate ettevõtete sertifitseerimisteenuste pakkumisega. Nimetatud organisatsiooni auditeerimisprotsessid kujundati ümber kasutades plokiahelat ning nutikaid lepingutehnoloogiaid, mille järel modelleeriti need kasutades CMMN modelleerimiskeelt. Analüüsimaks, kas CMMN modelleerimiskeel on plokiahelale tuginevate protsesside modelleerimiseks sobilik, kasutati raamistikku, mis hõlmab üldlevinud mustreid, mis on omased plokiahelale tuginevatele rakendustele. Selle tulemusena ilmnes, et CMMN modelleerimiskeele abil on võimalik plokiahelale tuginevaid protsesse üldiselt adekvaatselt kirjeldada, küll aga on siiski puudus elementidest modelleerimaks täpsemaid plokiahelatele ning nutikatele lepingutehnoloogiatele omaseid detaile.

Võtmesõnad:

Blockchain, CMMN, Äriprotsesside mudelid

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Table of content

1. Introduction

Blockchain technology became well known and acknowledged when cryptocurrencies like Bitcoin were presented [1], however, this is only one of the possible applications. This platform technology [2] has been speculated to be "the most important invention since the Internet" [3] and to be able to deliver significant business value for both financial and non-financial industries. That is why, companies in various areas start to use blockchain in their business processes. For example, banks and other financial institutions are highly influenced by this technology. It was claimed [4] that blockchain could influence bank's infrastructure costs related to cross-border payments, regulatory compliance and securities trading with saving up to $20 billion per annually by 2022. Besides the financial industry blockchain is being used in domains like healthcare, identity management, supply chain management, voting, real estate, authorship and ownership, etc.

Blockchain is a distributed database where every party that represents a node in the system can verify the records of the transaction's partner without a middleman that provides more trust [5]. The data in blockchain consists of transactions that are stored in blocks. While appending a new block it is linked to the previous ones that makes a chain of blocks [6]. As blockchain is a distributed database it means that there is no one storage of a data, but all the nodes hold all data within a system. Absence of a third-party, access to transactions, connections between different blocks and storage of all up-to-date records on a large number of participants ensure such qualities as transparency, traceability and immutability of data [7].

The companies have begun exploring how blockchain can be used in their processes, however, there is a question of how to implement and to adopt this technology for gaining positive results from changes. Commonly the new technologies are implemented to automate certain parts of the current process that affects the performance of the whole process. However, if there is a lack of communication between parts of the process it may interfere with process improvement. That is why a simple substitution of a current process with new technology would not be able to provide significant business value and the business processes should be changed with the peculiarities of new technology such as blockchain. For this purpose, a process redesign is used [8]. Such redesign requires a representation of the changes and a clear understanding of how the processes are that can be done via process modeling [9]. The process of redesign begins with capturing of the processes of the company, how they are right now ("as-is" model) and analysis of them. Only after having a model of the current situation suggested changes for redesign are estimated and are reflected in a new model ("to-be" model). Next steps of the redesign are an implementation of the changes and process monitoring. In the case of emerging new issues, the cycle repeats from the beginning [10]. Thus, modeling business processes is important for the analysis of the processes especially in the context of utilizing new technologies.

Business process modeling is used to graphically represent how the organizations operate. It is also considered as an important technique for process analysis, design of process-aware information systems and re-engineering [11, 12]. While modeling the internal processes either activity-centric approach, for instance, BPMN [13], either artefact-centric approach like CMMN [14] can be used. The artefact-centric approach focuses on the data that is manipulated and transferred within a process [15]. CMMN being a representative notation of this approach deals with cases where activities can be performed without a particular order and without particular performer being specified, but according to circumstances or conditions.

CMMN was chosen for exploration of this topic due to two reasons. Firstly, with modeling blockchain-oriented processes might be particularly applicable. The fundamental focus of blockchain is on data that is added on a chain and shared between participants [5]. Data-centricity is the core of artefact-centric modeling language such as CMMN. Moreover, authors [16] discussed that certain qualities of CMMN such as modularity, hierarchy and declarative characteristics of this modeling language may be particularly useful when representing smart contracts. Secondly, among other artefact-centric modeling languages such as Vortex workflow [17], CMMN is the standard adopted by OMG as of May 2016 [14]. Although BPMN has been used to model blockchain-oriented processes [18, 19], the suitability of artefact-centric method has not been investigated yet. In this context, the suitability of CMMN is explored for processes running on a blockchain system. In light of this, this thesis addresses the following two research questions: (1) How can CMMN, representing artefact-centric modeling language, be used to model blockchain-oriented processes? (2) What are the strengths and weaknesses of the CMMN in regard to modelling blockchain-based solutions?

In this paper, the capability of CMMN to model the processes running on a blockchain platform with smart contract technology is presented. The results of this paper contribute to the understanding how blockchain-oriented processes can be modeled with CMMN and what is the suitability of CMMN for such processes. This paper also creates a knowledge base for further investigations of this question. The research in this paper is useful for the process analysts engaged in the redesign of the processes related to the implementation of blockchain systems. The findings of this paper could help in deciding whether to use CMMN or not and how to use this notation when modeling processes on blockchain platform. This paper is based on the case study of the international non-profit organization providing the certification services for the companies trading the timber-related products. Particularly, the timber-to-charcoal process is explored in regards to the auditing process. In order to analyze and evaluate the capability of CMMN, the collection of patterns for blockchain-based applications is used [20].

The remainder of the paper is structured as follows. Section 2 introduces some background on blockchain technology including concepts of smart contract, token, and oracles. Another part of background includes giving an overview of CMMN. Section 3 presents the case study followed by the findings in Section 4. Finally, the conclusions are presented in Section 5.

2. Background

In this section the theoretical background is presented. It includes blockchain technology with necessary notion such as smart contracts, token, oracle and different types of blockchain. In this section an overview of chosen modeling language – CMMN is also presented.

2.1. Blockchain and Smart Contract Technology

Blockchain is a distributed database storing all the transactions that have been executed between participants [21]. Blockchain structure consists of blocks with the transaction information which make a sequence – chain of blocks. Every block has a block header and the block body. In the block header certain information is stored: block version (shows the set of block validation rules to follow), hash value of the transactions in a block (output of a cryptographic hash function), timestamp (current time), nBits (target threshold in encoded form), Nonce (the number added to a hashed block, blockchain miners and Parent block hash (hash of the previous block). The body of the blocks consists of transactions information: transaction counter and transactions themselves. This information guarantees the traceability of the transactions [22].

However, in order to record the transaction, the majority of participants in the network must verify and agree to add it on chain as there is no one centralized authority. Only after this approval the block can be added. After adding the block, it can no longer be changed and thus become immutable. Everyone can become a participant in the network, so the problem of the trust appears. This is an analog of Byzantine Generals (BG) Problem in the distributed systems [23] where the decision or agreement should be reached among the participants. It is relevant for blockchain platform as there is no central node to guarantee that ledgers on distributed nodes are the same. To solve this problem the consensus protocols were presented to have the rules of the agreement between different nodes. The most frequently used consensus approach is PoW (Proof of Work). PoW is used in Bitcoin where the right to record the transactions is given to the first node who will solve the math problem and find a hash value that refers to the block header [24]. There are other consensus protocol such as PoS (Proof of Stake), DPoS(Delegated Proof of Stake), PBFT (Practical byzantine fault tolerance), Raft, etc. They differ in a way how consensus is reached to add a new block and demand different calculation efforts. For example, PoS is less computer calculations demanding as the node should prove the ownership of the amount of the currency depending on the coin age [22].

Another important aspect of blockchain is a digital signature that ensures the security of the transactions. Each participant has two keys: private and public. The private key is confidential and is used to sign the transactions. Firstly, the hash value will be generated from the transaction and with the private key it will be encrypted. The encrypted hash value with the original information will be sent to the receiver who can verify the data from the transaction. Later the signed transactions are distributed to all nodes. The public one is used during the verification phase when the transaction is already signed by an initiator. The receiver can decrypt the hash value using the sender's public key with the hash value from the received data. After the verification of the transaction it is recorded and becomes immutable [25].

Blockchain enables the elimination of the trusted third parties like financial institutions that are needed to validate any transaction. That intermediate step causes higher transaction costs. However, there are other key characteristics of blockchain that influences investigations of this technology in other fields.

- *Decentralization.* The central trusted third-party for validation the transactions is eliminated. All participants have the same rights;
- *Persistency*. Every transaction is spread across all the network so that is stores on every node
- *Anonymity.* As every user is working with the blockchain using a generated address;
- *Auditability.* It is easy to trace and verify previous transactions as they go through the validation process and have a timestamp [22]

Blockchain enables the usage of smart contract technology. Smart contracts represent scripts of code that allow having basic computation on the blockchain. They give an opportunity to express business logic in code that will be run on blockchain and that is efficient, transparent and tamper-proof [26]. The advantages of smart contracts include the elimination of trusted central authority and automated execution across all the nodes according to the predefined conditions [27]. These predefined conditions ensure the precision due to prior agreement between involves parties and transparency as the conditions are visible and verifiable by all participants. The tamper-proof characteristic of the smart contracts guarantees that they cannot be modified or cancelled [28]. The first platform where they were introduces was Ethereum [29]. Application areas of smart contracts include financial, notary, loan, insurance and other domains.

Within the smart contracts there some particular concepts that should be described. The first one is a concept of the token. Tokens represent the variety of goods and are needed to keep track of an ownership and a transfer it to others i.e. are digital assets [30]. They may represent as physical goods or access rights like software license or subscription. Tokens can be managed by smart contracts that could provide more transparency of trading and help to eliminate frauds or corruptions as the ownership is stored on blockchain.

Another important concept is an oracle. Blockchain is a closed environment that does not interact with external systems. It means that importing or exporting information from the blockchain system is not provided. However, for the businesses it is essential to have the message exchange with the external world to receive the information and retrieve it from blockchain. To solve this problem the concept of the oracle was introduced. This is a connector that can receive the information from outside of the blockchain system and evaluate the conditions written in it [31].

Blockchain technology can deliver business value for business sectors [32]. For instance, blockchain technology is explored in use cases for e-governance where it is discussed to be a platform for serving transparent voting and providing citizens with different public services. In China, for example, the blockchain system was introduced to verify data origin and genuineness during the submission into the e-government and public services [33]. Another use case is healthcare. Blockchain can be a platform for storing and sharing the health data of the patients ensuring the privacy and security. There is already a functional prototype for managing health information – MedRec where patients share their medical information to doctors and health providers [34]. One more application area is energy. Blockchain technology enables to have transparent transactions for the energy market between consumers and providers [35]. With a blockchain technology it is possible to trace the product provenance and also the product ownership is recorded that is applicable for

supply chain domain [36]. Banks and other financial institutions also use blockchain to increase efficiency and simplify their transactions. As example can be a system "Ripple" that helps to complete the process of cross-border payments in 10 s instead of 2 days [37].

2.2. Types of Blockchain

There are three types of blockchain: public, private and consortium [38]. The main difference between three types is that public blockchain is fully decentralized, the consortium is partially decentralized, however, the private one is fully centralized and is controlled by a single organization or a group. This implies that in the public, non-permissioned blockchain systems everyone having access to the Internet can send and see the transactions. As an example, can be the cryptocurrencies like Bitcoin or Ethereum. In a consortium blockchain system, there is restricted access to participants for verifying of the transactions. For this purpose, there is a pre-defined group of nodes in the network who should verify the transaction before it will be stored. Such systems are used by banks, for instance, R3 consortium [39]. In private blockchain write permission for the transactions is left to only one organization. Such systems are used for internal purposes of the company like data management or auditing. The read permissions for private and consortium blockchain may be public or restricted [22]. Taking into account all benefits blockchain offers it should be noticed that there are some weak places of this technology in terms of using it in the business. One of the main concerns is the scalability of the solution based on blockchain. Public blockchain has a limited capacity of recording blocks that affects the time and costs of processing the transaction. For Bitcoin throughput it is 7 transactions per second [40]. However, private blockchain systems can be scalable due to a limited number of participants in the network [41].

Apart from the advantages of blockchain-based systems, there are several concerns and the biggest one is scalability as the number of transactions increases every day [38]. Firstly, because of the structure of blockchain and need to store the block size has a limited capacity of storing the transactions. Secondly, all transactions are saved on each node to validate them. Thirdly, there is a time delay for generating a new block. This causes a technical issue of scalability of public blockchain systems and also influences time and cost for processing the transactions. As the blocks after validation are linked to the previous ones to ensure the immutability of transactions it also causes the problem of data storage [22].

There is another important aspect – transactional privacy as in blockchain the values of transactions and balances that are linked to public keys are visible to all participants [42]. This is especially important for the private blockchain systems, where participants have a risk of revealing their commercial information. In order to solve this problem of data security encryption process could be used. Encryption ensures that only participant with a private key will be able to decrypt the data i.e. the privacy of the data in transactions is controlled.

One of the examples of private blockchain is Fabric – an open-source platform that offers private blockchain. It is one of the projects of the Hyperledger [43]. Fabric is already used in different production distributed ledger systems in various areas. Fabric is the first blockchain system that can work on the application written in standard programming languages (Java, C++, etc.) in a way that they can be executed consistently on several nodes [44]. The nodes in the network are divided into two groups of peers: validating and non-validating. The former has the right to run the consensus, validate transactions and maintain the ledger. The latter is needed to connect the client with the

validating nodes. As it is a permissioned blockchain in order to connect to the network the enrollment certificate is necessary. Another certificate – transaction certificate - is needed to be authorized to submit the transactions in the network. Privacy of the data is guaranteed by the systematic encryption of the transactions [45].

2.3. Modeling language

For the business modelling the common standard is the Business Process Management and Notation (BPMN) by Object Management Group (OMG). It is suitable for the processes with a defined flow of activities. However, more and more attention was paid to the knowledge workers and flexibility in the business processes where, for example, exceptions may occur or the activity flow depends on decisions of a worker. The problem of modelling such processes led to publishing in 2016 Case Management Model and Notation (CMMN) by OMG and now became another standard for modelling business processes to serve unpredictable processes that need more flexibility [14]. In the core of CMMN there is a need to support case management and its handling i.e. to model the activities that are not repeatable or pre-defined as well as are not well-structured. This means that activities depend on the circumstances, outside events, results of other tasks and decisions by knowledge workers.

2.3.1. Case Management Model and Notation Specification

The most general element is the concept of a Case. Case Management itself was created to help different agencies to deal with customers and every interaction was considered as a Case. In the specification, the Case is a process where the actions are taken to achieve a goal. There may be standard or predefined paths, however, the knowledge worker processing the Case can decide whether to perform some tasks according to his/her evaluation. Traditional examples are a lawsuit, insurance claim, patient record, etc. The individual Cases can be solved fully in an ad-hoc manner, however, with time and experience the common patterns may be seen. This became the practice of Case management – to process and solve Cases that got the name of "case handling" [46]. While designing the process model the plan for the execution of the case is created. The steps for handling the case are added that are predefined or "discretionary" that are available for the knowledge worker according to some circumstances. However, during the run-time phase, the information coming to the worker influence the case execution, so he or she can add discretionary tasks to the particular case. For instance, in a claim management (see Figure 2) there are tasks without which a claim cannot be processed and there is a set of tasks that may be performed when needed. Being a declarative notation, CMMN describe what should be done or achieved instead of stating how it should be done.

As CMMN is an artefact-centric modeling language it focuses on the flow and manipulation with data. All the data needed to process the Case is represented by the CaseFile. It represents all type of data: documents and other structured and unstructured data. CaseFile may serve as a context for proceeding to other tasks or for evaluation expressions. Information in the CaseFile is also used as a case parameter for entry and exit sentries.

Case plan model captures the complete behavioral model of a Case. A Case plan model can include such elements as tasks, event listeners, milestones and is organized in stages. Tasks represent a defined part of work such as human task, for example. To capture the time or user event during the case execution the event listener should be used. Milestones serve as a goal that should be achieved and for the evaluation of the case progress. An important role plays Criteria that represents conditions for the beginning (entry criteria) or terminating (exit criteria) of the tasks, stages or a case plan. Criterion should be written in sentries and can be placed on the border of the case plan elements. For the milestone sentries represent only a condition for achieving it. Sentries are used to show the dependencies between plan elements. For example, competing of one task enables the beginning of another [47]. In CMMN there is no defined flow of activities as the execution of the tasks depends on different conditions and events. That is why sentries can be used to show the sequence of activities according to the circumstances.

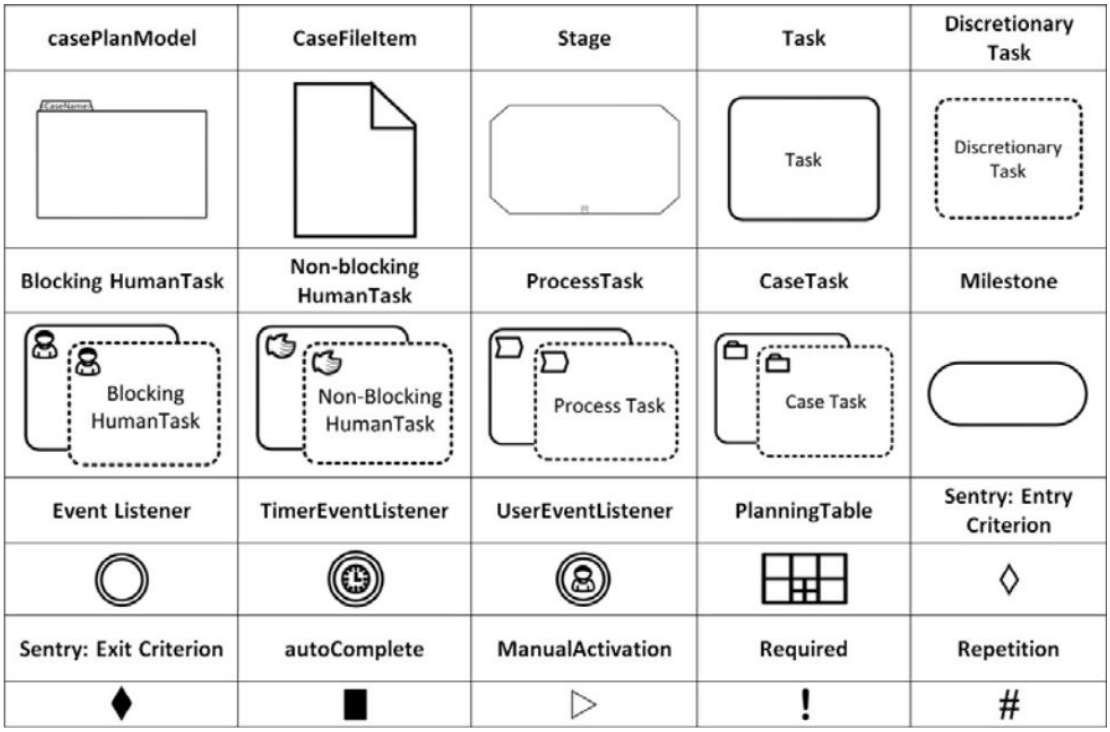

Figure 1. Visual CMMN elements [48]

On the Figure 1 the elements of CMMN are introduces along with the decorators that can be added to the elements.

2.3.2. Example

Figure 2 illustrates the claim processing modeled with CMMN. It is a knowledge work and can be performed in different ways. Process has three milestones (Responsibilities Identified, Base Information Attached, Claim Processed) that should be reaches. Some tasks (Change Responsibilities or Create Letter) are left to the discretion of the worker. Some tasks (Identify Responsibilities or Create Claim Notifications) are mandatory for execution that is represented with a decorator. Another

set of tasks (Request Missing Documents or Review Documents) have a repetition rule represented by a decorator. The process will finish by decision of the worker (User Event Listener) or when the Claim is processed. In there was a need to show an event related to the moment of time – Timer Event Listener would be used.

When the process is quite complex some sub-processes can be generalized as one task in a high-level model. In a current example some tasks are process tasks (Identify Responsibilities, Request Missing Documents and Create Letter) or case tasks (Create Claim). Process tasks represent another process that may be modeled with BPMN and case tasks refer to another case plan model.

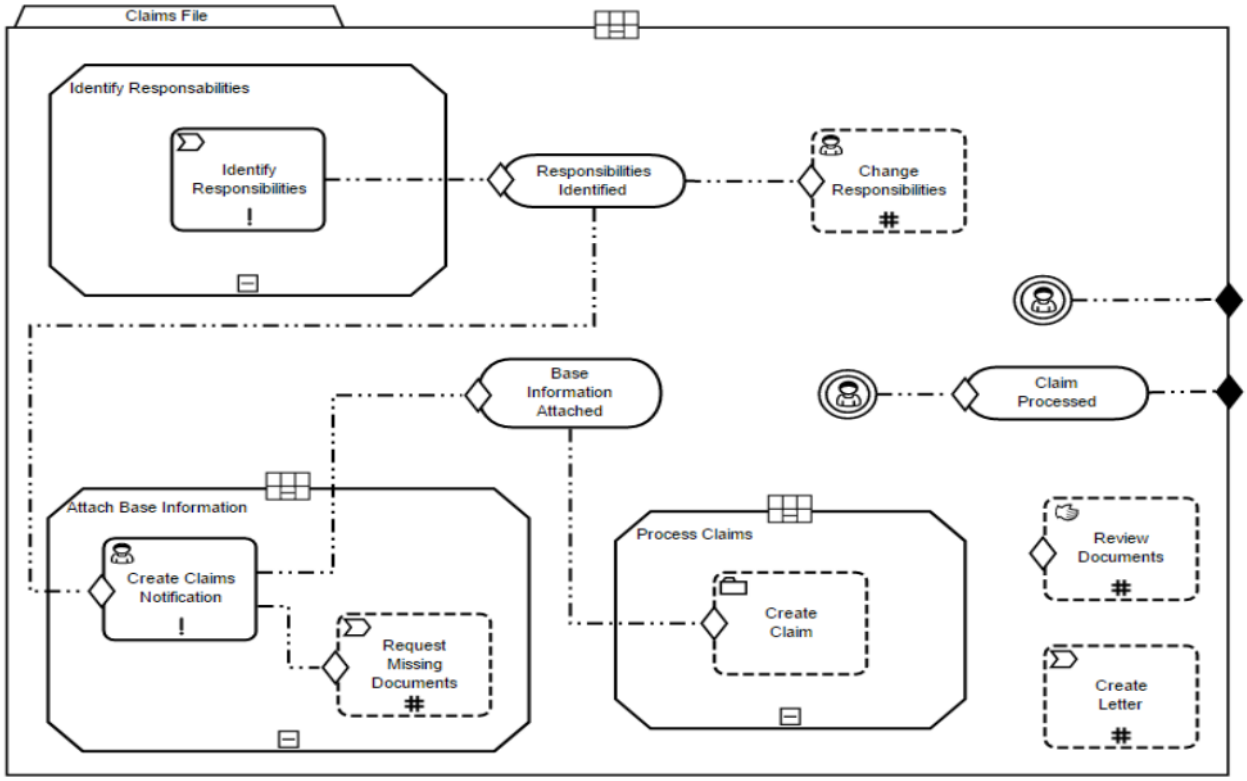

Figure 2. Claims Management Example [14]

It should be mentioned that the order of the elements does not affect the execution of them. Dependencies of the execution are shown by the connectors and sentries.

3. Case Study

In this section the selected research methodology is presented with the description of the method and general steps while conducting it. After the execution of a case study is described. Also, the overview of a current timber-to-charcoal process and its redesign based on a blockchain solution is presented.

3.1. Case Study Research Methodology

The case study methodology is used in various fields where the deeper understanding of studied phenomena is needed. By combining qualitative and quantitative data analysis it allows to study the data in a specific context. As case study is always connected to the real-life events it has a high level of realism. A case study method is used by researchers to explore the interested phenomenon, to explain it (which may include the test of the hypothesis) or to describe it by the data received during the case study [49].

There are different purposes for conducting a research. According to the Robson (2002) [50] the classification includes four aims: exploratory (to figure out what is happening, provide insights and hypotheses for a new research); descriptive (to depict a situation); explanatory (to interpret a situation, find explication of what is happening); improving: (to improve a certain aspect of a studied situation).

It should be noticed that no one research methodology on its own can serve all the purposes at the same time. Originally, the case studies were used for exploratory purposes. However, it also can be used for descriptive or explanatory purposes. The latter can be related to the testing of the hypothesis. In a software engineering the case studies are also used having the improving purpose, for example, the QA study [51].

An important notion in a case study method is a triangulation that means to study the phenomenon from different angles to provide the bigger picture. According to the Stake (1995) [52] there are four types of triangulation that can be applied: data triangulation (usage of more than one source for the data collection), observer triangulation (usage of more than one observer), methodological triangulation (combining different methods of data collection i.e. quantitative and qualitative methods) and theory triangulation (usage of different theories).

Case studies are now used not only in social science but in software engineering as well. Case study allows to study a situation or a phenomenon in their context and is particularly useful when the boundary between the environment and the phenomenon is unclear. This is applicable to the experiments in a software engineering when there are many factors that affect the outcome. That is why the case study research method was selected for this study as apart from the given context there are factors related to the implementation of new technology, its adoption, communication and trust issues between parties that should be taken into account. This is commonly used purpose of case studies – to explore the topic. It allows to gather necessary information about the case (auditing within timber-to-charcoal process) with deep understanding of the context (Nepcon - chosen an international non-profit organization) in order to address the unit of analysis (blockchain-based solution with CMMN). In comparison to other research methods like surveys, case study gives information about

the process by means of data triangulation or experiments, case study does not imply an experimental control that was not needed for this study.

The case study process follows the steps of almost any empirical study, for example, proposed by Wohlin et al. (2000) [53] and Kitchenham et al. (2002) [54]. As a case study is a flexible research method that means a planning is not necessary, however, it is suggested to be done to conduct a successful case study. In general, there are five major steps while conducting it:

1. Case study design: the case study is planned, and specific objectives are set;
2. Preparation for data collection: procedures for data collection are defined;
3. Collecting evidence: execution of a case study with data collection;
4. Analysis of collected data;
5. Reporting.

For this case study, the general process described above was followed. Firstly, the case study design was defined including objective of the case study, research questions and case setting (what exactly is being studied i.e. what kind of company, department, etc.). Then the data collection methods and procedures were discussed. After that the execution of a case study took place when the data was collected. Finally, the analysis and reporting were done. More precisely the case study is presented below.

3.2. Case Study Design

3.2.1. Objective

In this paper the case study method was used to explore the research question of how the CMMN modeling language can be used to represent the blockchain-oriented processes. This topic was not well investigated before therefore this research paper could provide the knowledge base for its further exploration.

More specifically the research questions are formulated as follows:

RQ1: How can CMMN, representing artefact-centric modeling language, be used to model blockchain-oriented processes?

RQ2: What are the strengths and weaknesses of the CMMN in regard to modelling blockchain-based solutions?

A case study method was chosen first of all according to the need of blockchain-oriented solution. However, given the research questions there are also two criteria for the case that should be fulfilled:

a. The case should be suitable for executing on the blockchain-based applications,
b. An access to the information is provided by domain experts and documentation.

Taking into account these criteria the timber-to-charcoal process was chosen for the case study. The selected process fulfils the first criterion of being suitable for blockchain-based solution. The part of the auditing process is done by comparing the invoice data of the company with the respective data of its supplier/buyer. The exchange of confidential data (invoices) during the auditing

process requires a solution that can guarantee trust in terms of protecting this data. The second criterion is fulfilled as the necessary documentation and access to the domain experts was provided. This gave sufficient information for conducting a case study.

3.2.2. Case Setting

For the setting of the case study was chosen an international non-profit organization Nepcon (Nature Economy and People Connected) [55]. Nepcon offers the certification of the wood products and training services related to sustainable development in a wood industry. In return, to have a possibility to certify other companies, Nepcon is certified by ASI [56] (Assurance Services International) an organization that verifies a compliance with the sustainability standards. As blockchain is being investigated for usage in supply chain [57, 58], where it gives an opportunity to accurately trace the goods from the producer to the end user, such companies as Nepcon could benefit from this technology to reduce a manual work and a possibility to cheat from the side of a company that is being certified. Also, Nepcon has already investigated the potential usage of smart contracts on permissioned blockchain in their processes, however, it was not yet implemented. That is why Nepcon was a suitable object for the case study as the blockchain-oriented solution was discussed and the models of a business processes for it were needed.

One of the main areas of activities for Nepcon is certification of the companies that produce or are engaged with the trade of timber and timber-related products. The companies need this certificate to comply with the regulations in such markets as USA, Eu and Australia. This case study is focused on the auditing during the timber-to-charcoal process that starts with the wood owner and finishes with the end customer which makes this a single case study. This process (timber-to-charcoal) was chosen due to its representativeness of the Nepcon's auditing process that is fairly the same for the other processes. Furthermore, during the timber-to-charcoal process the materials change their form completely that make it difficult to trace them within the process. Additionally, an exchange of commercial documents (volume reports and conversion rates) takes place within the auditing process. This information cannot be stored in centralized database as there is a risk of being publicly disclosed. All mentioned above make this process suitable for a blockchain-based solution with usage of smart contracts that ensures data security when there is a lack of trust between participants.

3.2.3. Data collection

To conduct the case study the deep understanding of the process is needed to represent it with the model and then redesign the process. To capture all the details data triangulation was used i.e. several data sources. Firstly, the direct method – interview – was used to collect necessary information about the timber-to-charcoal process. The interviews were used as an expert knowledge was needed for deeper understanding of the process, its requirements and limitations for redesign as well as for the verification of the solution. Nepcon representative, Roman Polyachenko, Director of NEPCon Estonia and Chain of Custody Program Manager, has attended several conferences dedicated to blockchain and smart contracts that is why he is familiar with blockchain technology that was an advantage of conducting interviews with him and discussing a potential solution on more technical level. Another method included independent analysis of the provided documentation by Nepcon. A

set of documents was given by the Nepcon representative for deeper investigation of the process. This set included example of the audit report, example of a certificate issued by Nepcon, example of annual volumes summary template and Nepcon certification procedures document where the audit procedure is described in terms of conditions for receiving a certificate, mis-conformances management, suspension process, etc. As the provided documentation is related to a specific company that was certified by Nepcon and contains the confidential information about the company's performance, the ethical aspect was taken into consideration. The information that refer to the company such as the name, address of a company was deleted by Nepcon before providing documents.

3.3. Case Study Execution

The execution of the case study includes several steps:

1. Workshop to map "as-is" process. The initial workshop was held with Nepcon to discuss the timber-to-charcoal process in general and create a simple visualization of it using drawings. As well the process of the supply chain in general (from forest owner to the end customer) was discussed and a conceptual model was created. The chosen notation (CMMN) was not used during the workshop in order to avoid biases as another modeler had to use different notation – BPMN.
2. Modelling of "as-is" process. After the workshop the visualization of the process was transferred to the business process model using CMMN. During this step additional documents were provided by Nepcon to capture all necessary details in the model. The drafts of the model were discussed with the Nepcon to verify and refine unclear moments and the final version was also reviewed by Nepcon. While modeling the "as-is" process there was no cooperation with another master student and the models in CMMN and BPMN were not shared to avoid biases.
3. Redesigning of the "as-is" process. Having the current process modelled the workshop with Nepcon was conducted to discuss a blockchain-oriented solution. During the workshop the requirements of the solution were decided considering the limitations. The conceptual model of the blockchain-based solution for the process was made. The formal notations were not used during this workshop as it was with the first one.
4. Modelling of the "to-be" process. Based on the workshop's output the model for the "to-be" process was created. This step follows the process of the second step. The final version of the model was verified with Nepcon.
5. Analysis and evaluation. The modeled business process was analyzed in regard to using the CMMN for the blockchain-based solutions. For this purpose, the framework of patterns for blockchain-oriented processes was used [20].

In total there were 6 interviews that lasted around 90 minutes each. These interviews included initial meeting were the details of the project were discussed, interviews for understanding the current process, interviews for redesigning and presentation of the results. The interviews with the Nepcon representative were semi-structured as there was a set of predefined questions, however, according to the answers some of them were not asked and the other ones were asked additionally to the list. During the interviews all the members of research group could participate that ensured observer triangulation. Apart from 6 interviews with Nepcon several meetings were dedicated to the modelling part. During these meetings the questions of capturing process details in particular notations were

discussed with the supervisors. As another modeler was working on the same subject modeling the process with BPMN the meeting for each notation were conducted separately to avoid biases and only conceptual models were exchanged.

Finally, the documentation of the created models for the current and redesigned process was done (Section 3.4) as well as analysis in regards to research questions (Section 4). The last step – reporting of a case study is presented as this research paper.

3.4. Timber-to-charcoal process

This section describes the timber-to-charcoal process firstly as it is and reasons for it redesigning. Then, the proposed blockchain-based solution is presented.

3.4.1. The "As-is" process

The certificate is needed for the companies operating in the wood industry to be able to sell the certified timber and timber related products i.e. with certificate logo attached to the package. In the timber-to-charcoal process there are several participants. The process begins with the forest owner who prepares the round wood that is later sold to charcoal manufacture either directly or via broker. The charcoal manufacture produces the charcoal by burning the round wood with the conversion rate for the industry on average 20%. The conversion rate differs among the manufacturers. The charcoal manufacturer sells the charcoal to the secondary producer who packs it. The conversion rate for the packing is estimated to be around 90%. Later the secondary producer sells the bags of the charcoal either directly to the end consumer that is represented by retailers or via bulk buyer (see Figure 3).

Firstly, in order to start the certification, process the company requests the inspection from Nepcon. The company and Nepcon should sign the agreement that gives the possibility for Nepcon to inspect the company for complying with the certificate requirements, for example, interview people, verify work conditions, have access to the internal documentation, etc. The certificate is valid for 5 years and requires an audit every year to confirm the validity of the certificate. The certificate status is saved in FSC database and is updated after audit.

The inspection process is divided to two parts: onsite inspection and inspection of the documentation. During the onsite inspection the expert from Nepcon visits the company's workplace and performs the audit according to the pre-defined checklist that should be filled in. Documentation check includes also the verification of job and safety instructions, reports, etc. Another important part of the audit is to assess the volumes of the timber that company buys (income) and sells (outcome). This is done by the Nepcon expert manually. The auditor inspects the invoices that company provides with the summarized volumes report also provided by the company. The expert should verify that outcome volumes are reasonable according to the conversion rates and the income volumes. If there is a need for more detailed check the inspector can ask for real invoices (see Figure 4).

After the inspection the administrative work is performed when the expert should assess all received information and write the report with the proposed decision. Another Nepcon expert reads the report and should confirm the decision. When the decision is made it is submitted to the official

FSC registry where it is possible to see all certified companies in the industry. The certificate can be also issued despite the small mis-conformances (less than 5) founded during the inspection. In this case the company will have time to solve the existing issues and an additional audit is scheduled to inspect problem areas.

The current auditing process has several disadvantages. First of all, because of the paper invoices there is a space for a fraudulent activity that cannot be detected by the expert. Moreover, the documents for the audit are prepared by a company that gives a possibility to show wrong figures. The company can hide information or modify the volumes in the invoices intentionally. For example, the company sells in real life the timber as certified not buying it enough but replacing it with not certified. Another issue is that the manual process does not allow to verify all the invoices and make a cross-check them with the invoices from buying and selling companies. Taking into account that the audit is scheduled and is conducted every year at approximately the same time, the company is prepared for it. All listed above may led to the occurrence of the frauds without being detected before the next audit. As the audit is done only once a year it means that the company can operate for as long as year not meeting standards before the expert can detect it and suspend the certificate. It also means that the suppliers' certificate is checked with FSC database once a year during the audit that may lead to buying not certified timber products for a client company. This is a risk for its operations as the materials will be sold further as certified probably not meeting the standards. This affect the whole chain of the timber-to-charcoal process and lead to the trust issue between the participants. Speaking about the trust, the companies in the chain try to protect their internal data and resist using IT solutions based on central databases because of fear of data breach. The mentioned disadvantages of the manual audit processing stimulate Nepcon to find possibilities to improve it and were used as a basis for the requirements for a blockchain-oriented solution.

The supply chain in general is presented on Figure 3 and the auditing in a timber-to-charcoal process is shown on Figure 4.

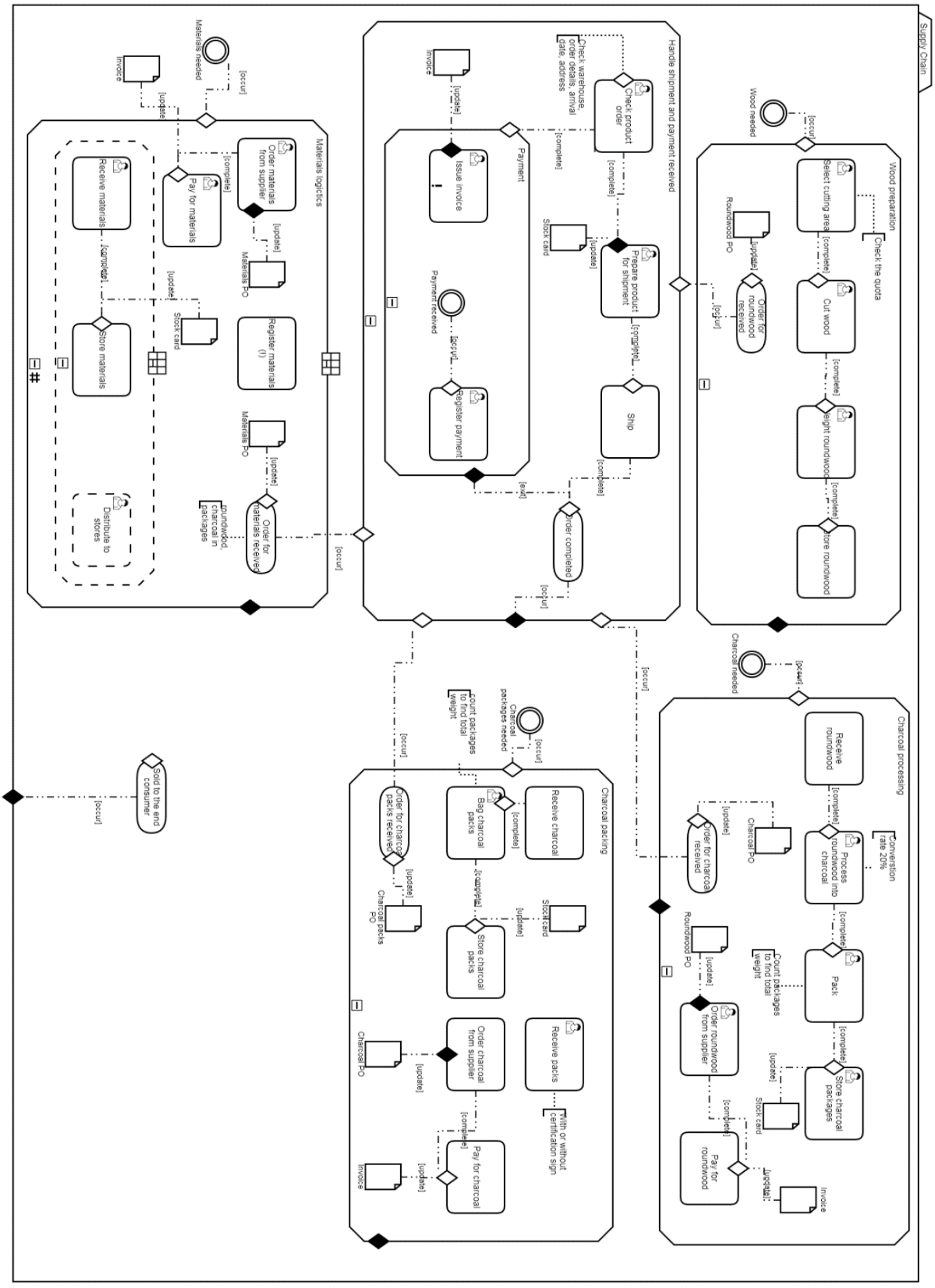

Figure 3. Supply Chain "As-is".

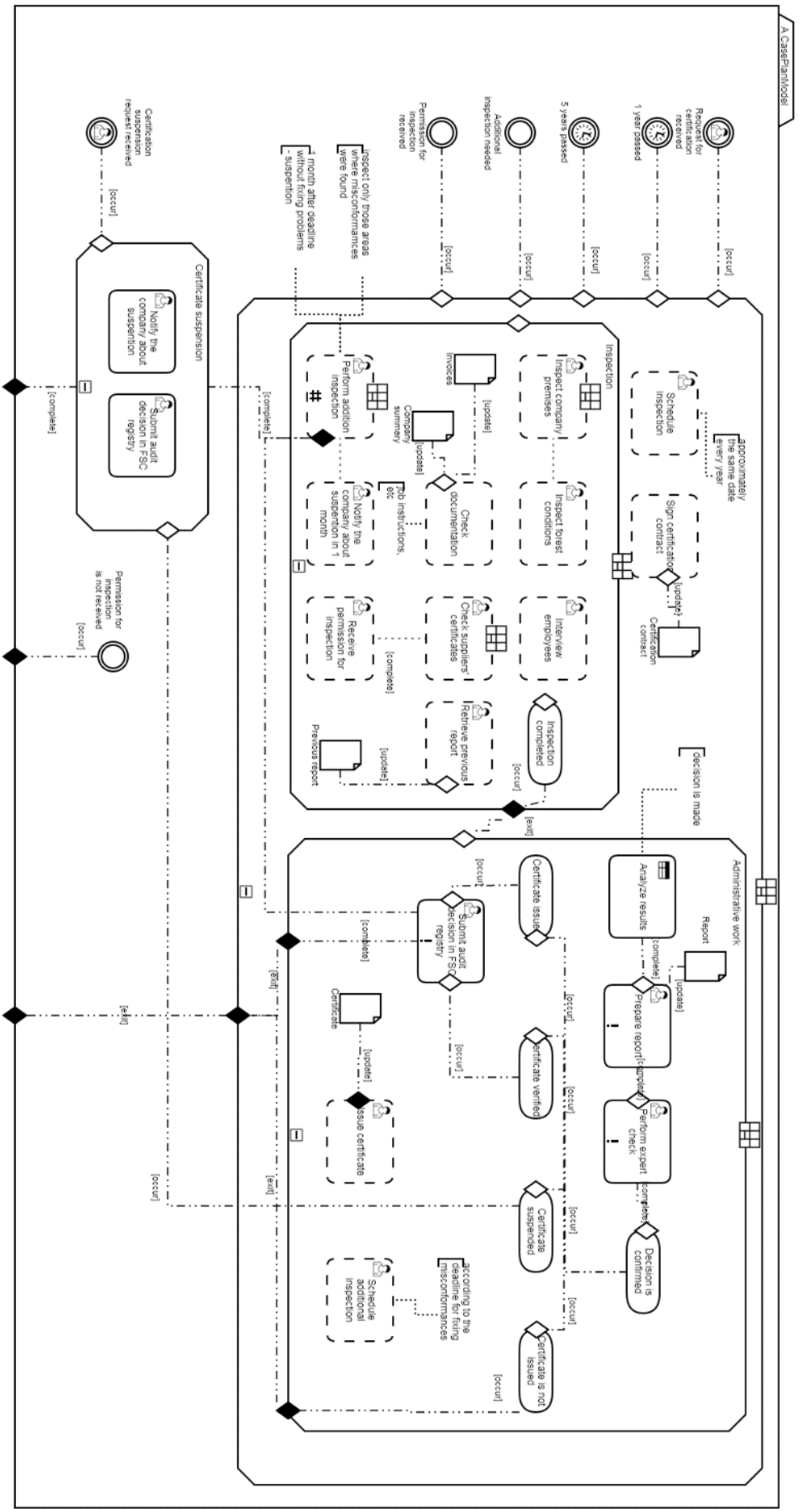

Figure 4. Auditing process "As-is"

3.4.2. The "To-be" process

In "to-be" process involves not only Nepcon but companies who want to be certified and other certifying organizations as well. These organizations will have access to one solution – permissioned blockchain system – that gives a possibility to inspect the companies even if their suppliers were certified by another company, for example.

The certificate confirms the right to trade the certified timber, but also shows the conditions of this trade i.e. the type of timber products. During the first auditing after the positive decision the certificate is saved on a blockchain system in a smart contract and represents the physical certificate digitally. The certificate can have different status (active, suspended) according to the status of the physical certificate. This process is modeled as an Onboarding process (see Figure 5).

After the digital representation of the certificate was created the company will have access to the blockchain system where it should upload the invoices related to the trade of certified timber. This is enabled by second smart contract *Invoice data entering*. The company can upload the invoices in a pdf format and in a special system *Invoice upload and hashing* the necessary information for the auditing (company name, seller/buyer, product type, volume, etc.) will be extracted and will be sent to blockchain (see Figure 6). The hashing of the invoices and extracted data is needed to ensure, firstly, the confidentiality of the information that cannot be accessed by everyone. Secondly, it guarantees that the invoices are not modified after being uploaded and the information saved on the blockchain system is the same with one that was uploaded with the invoices. Such a system for the document management between the companies and the blockchain system will be a third-party.

The parameter that expert refers to while auditing the company is a conversion rate. This parameter is different for every company and can change due to the improvements of the process. In the "to-be" process the companies can update their conversion rate by entering the new figure to the system. However, before updating it the automated verification will be done to check if it is within the industry range. In any case Nepcon has to review it and decide whether to approve it or not to exclude the fraudulent activity. This is represented as another smart contract *Conversion rate change* (see Figure 6).

As the main idea of the invoices' audit is to match the volumes in the invoices with the overall income and outcome volumes of the timber products, the aggregation of the extracted information from the invoices is introduced in the "to-be" process to automate the process. The aggregation of volumes also considers the conversion rates of the company. After calculation the aggregated volumes the check of fraudulent behavior is performed. If the amount of sold timber product is greater than the amount of bought timber product taking into account the conversion rate, it can mean an existence of a mis-conformance. Another automation is presented by explicit calculation of a conversion rate for each type of timber product given the volumes bought and sold by the company (see Figure 6). This allows to verify the real conversion rate with the one that is entered by the company and the industry range. If the conversion rate deviates beyond a certain threshold, it also can indicate a mis-conformance. In the case of potential mis-conformances Nepcon is notified for further investigation of the situation.

The results of the automated calculations and verifications can be seen in an external system that is represented by *Monitor*. In the *Monitor* Nepcon can observe the companies that were certified by them. The *Monitor* also sends all the messages to Nepcon that are triggered in blockchain. In case

of founded mis-conformances Nepcon will be notified, will investigate the situation and make a decision about the certificate of the company. Nepcon can change the status of the certificate in the system by means of *Token management* smart contract. If the status is *suspended* the company will no longer have possibility to upload the invoices in the system that means they no longer can trade the certified timber products (see Figure 6).

The analytical verifications (aggregation volumes verification) are proposed to be done on one analytical node and then the results to be populated on other nodes and therefore saved on blockchain. This will help not to overload the blockchain because of the intensiveness of the processing. It is suggested that ASI, certifier of the Nepcon and other similar organizations, has an ownership of the blockchain solution and the analytical node. It is also suggested to have scheduled verifications. For example, every three months the aggregated data of volume-in and volume-out is extracted to check according to the business rule (whether volume-in was greater than volume-out taking into account conversion rate). Another scheduled verification relates to conversion rate. Every three months according the volume-in and volume-out data the actual conversion rate can be calculated and checked with one that is reported by a company. The results of the verifications are saved in the database of the analytical node and recorded on blockchain.

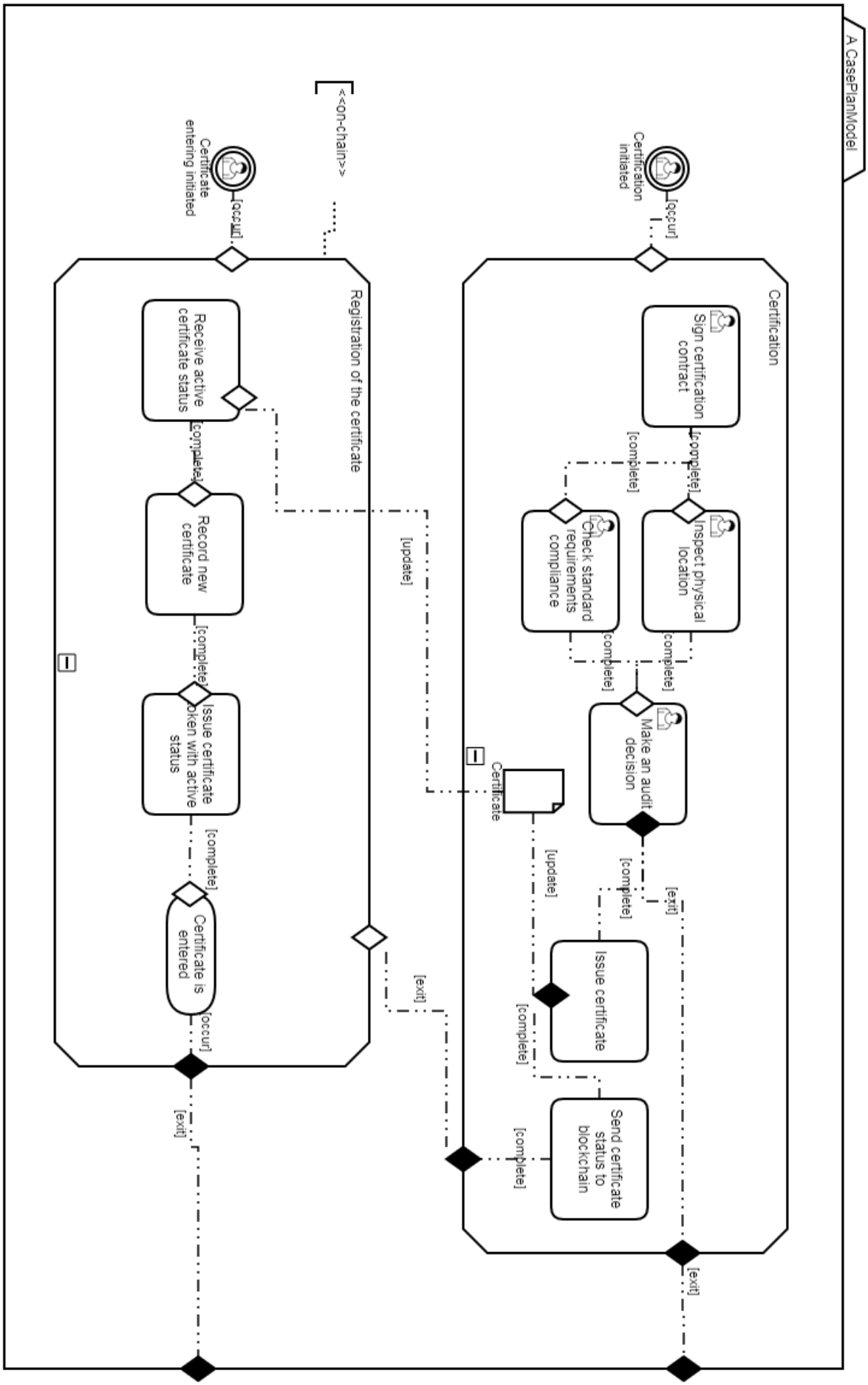

Figure 5. Onboarding process "to-be".

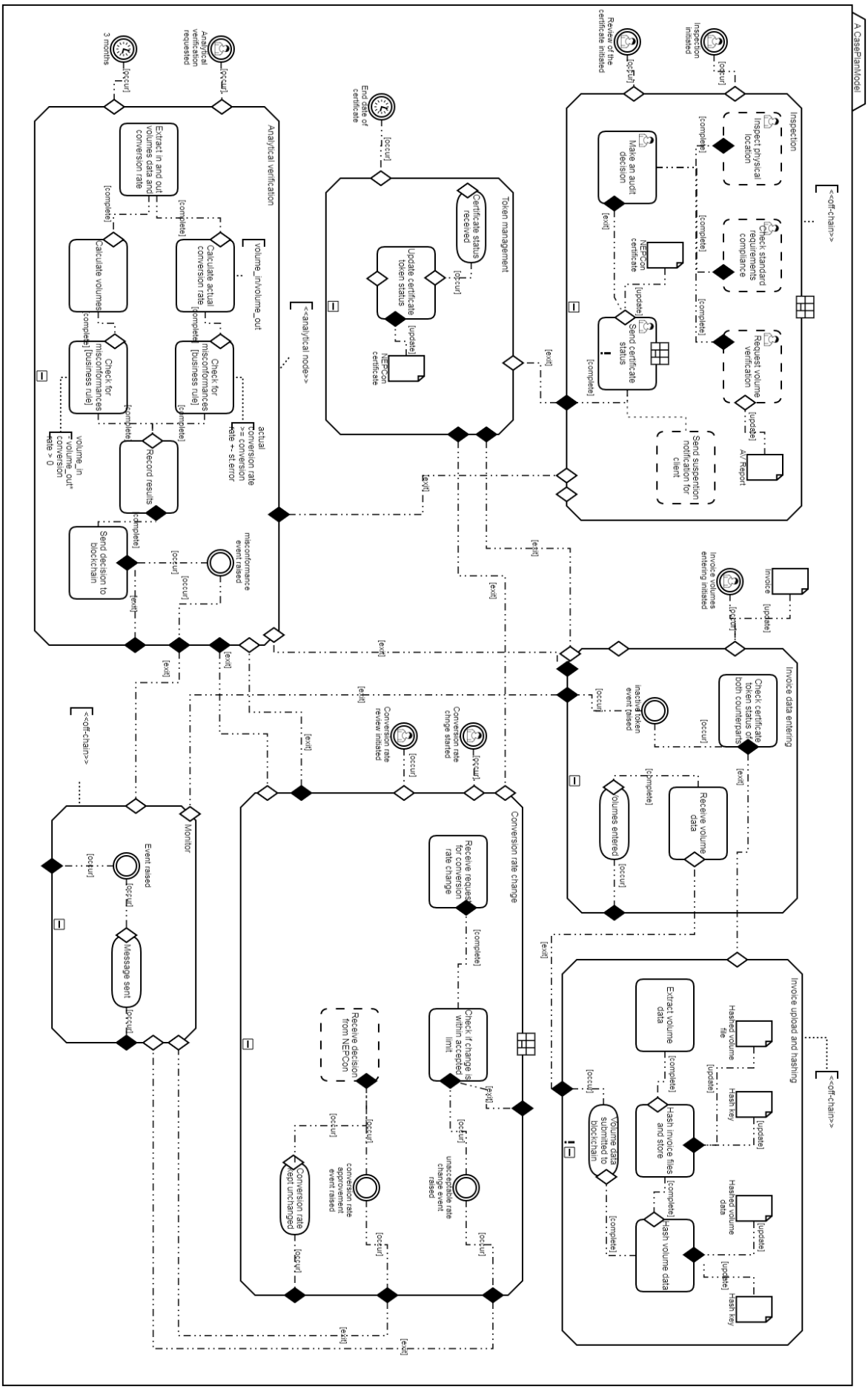

Figure 6. Auditing process "to-be".

3.4.3. Main changes in the process

The process was redesigned according to the problems that were discovered in a current process. With the introduction of a permissioned blockchain system, several issues were eliminated. Firstly, the paperwork of checking the volumes amount in invoices and summarized report was automated. This gives several advantages. It reduces opportunities of fraudulent activity from the side of a certified company as now volume data will be directly extracted from the invoice file and will be verified with the same data of another counterpart. The summarized report will be also done automatically according to the uploaded invoiced and the company would not be able to manipulate with that data. It also gives auditors more time and capacity to focus on other aspects of the inspection process such as physical premises, work conditions, etc. It should be mentioned that the physical onsite inspections remain without changes. With an automation the data is verified in real-time and in case of encountered mis-conformances Nepcon will be notified. Therefore, the delay between a potential violation and its expertise is reduced. It also applies to the suspension of the certificate. Now it will not be possible to trade with certified timber products with a suspended certificate as access to the system will be denied. It should be also mentioned that the certificate status is checked every time the company wants to upload the invoice that is why there will be no delay in trading after the suspension of the certificate. Secondly, the trust issue and security of commercial data are solved by usage of blockchain technology as everyone holds all data. However, the individual transaction details are encrypted and can be seen only with a special key.

With addressing the weaknesses of a current process new system also propose several additional improvements. As all the companies operating in this domain should be connected to the system for certifying companies like Nepcon it gives an opportunity to check client's data with its suppliers even if they were certified by another company. The possibility for intentional manipulation with conversion rate is also reduced by automated calculation of actual conversion rate and acceptable range. The summary of main changes is presented in table below.

Table 1. Main changes in a process

Current process	Proposed solution	Improvement
Volumes amount in invoices with summarized report is checked manually	Automated verification from uploaded invoices with results of aggregation smart contract	Less opportunities for fraudulent activity; gives auditors more time and capacity to focus on other aspects of the inspection process
Data is verified once a year during auditing	Data is verified in real-time and Nepcon is notified right after encountering mis-conformances	Delay between a potential violation and its expertise is reduced
Certificates' statuses are checked once a year during auditing	Certificates' statuses are checked every time the invoice is being uploaded	Access to the system will be denied with a suspended certificate
No access to data of companies certified not by Nepcon	Certifying companies are connected within one system	Possibility to verify data with suppliers certified by other companies

4. Findings

In this chapter the capability of CMMN for modeling blockchain-oriented processes is analyzed. Firstly, the collection of the fifteen design patterns for blockchain-based applications [20] is introduced as a basis for the addressing the research question. Then the representation of these patterns in CMMN is discussed along with a suitability of CMMN and threats of validity.

Design patterns are used to represent reusable solutions to common issues that occur in particular environment [59]. Xu et al. [20] created a collection of design patterns according to real-world blockchain-based and smart contracts solutions. These patterns also address architectural elements in blockchain-based applications and interactions between them. A set of these patterns represent common aspects for designing applications running on blockchain therefore it can be used for modeling blockchain-based business processes.

For now, there four groups of design patterns with fifteen patterns in total [20]. First group includes patterns for *interaction with external world* that describes the opportunities for blockchain-oriented solutions to exchange data with the real world. The second group cover the *data management* aspect. This includes on- and off-chain data management. The thirds group is related to the *security* aspects such as authorizations. The last group that is named *contract structural patterns* includes patterns related mostly to the technical side of blockchain-based applications such as reducing the size of smart contract code.

For this study only the first three groups were used for analyzing how CMMN can be used to model blockchain-oriented solutions. The fourth group of patterns was excluded as it is relevant for implementation of smart contracts whereas the focus of this study is on conceptual modeling that commonly does not include coding patterns.

4.1. CMMN Model Structure

The proposed solution is represented as one Case Plan with different Stages to show the sub-processes (ad-hoc). In this case the Case Plan captures the auditing process within the timber-to-charcoal process. As the proposed solution includes several systems where the processes are executed an alternative way would be to model each of these systems as a separate Case Plan. However, according to CMMN each Case Plan should be self-contained and give an overall picture of the process that is not possible with separating the solution into several Case Plans. Moreover, there are no relationships between Case Plans that also affects the understandability of the solution in general as in the redesigned process the parts are connected showing the flow between sub-processes. That is why one Case Plan is used to represent the solution. The proposed solution also implies the onboarding process to be done before. Therefore, the onboarding process is represented as a separate Case Plan. Interactions between subprocesses are represented by links and entry and exit sentries. Artefacts are modelled as Case Files. Annotations are used to clarify certain aspects, for example, where the subprocess is done on- or off-chain.

4.2. Patterns for Interaction with External World

Patterns for interaction with the external world consists of *verifier* (pattern 1), *reverse verifier* (pattern 2), and *legal and smart contract pair* (pattern 3).

Some transaction running on blockchain may depend on the state of external systems. Also, the external, off-chain application may need the information stored on blockchain for verifying conditions or computations. The problem with interaction with external systems is that blockchain can access only the information that is stored on blockchain. In order to connect the closed environment of Blockchain with external systems a concept of *Verifier* (pattern 1) and *Reverse-Verifier* (pattern 2) was introduced [20]. They represent a trustworthy third party to organize the information exchange e.g. to provide blockchain and the particular smart contracts with information from external systems to enable execution of functions on blockchain (Verifier) or retrieve the information stored inside blockchain to external systems. For better understanding the difference between these two it was decided to look from the point of who needs the data, but not from where the data comes. So, if the information is needed for the internal system running on blockchain it is a verifier; if the data is needed for external systems from the blockchain storage – it is a Reverse Verifier.

In our case several Verifiers and Reverse Verifiers were identified. The invoice upload and hashing process is a Verifier as an internal system based on blockchain needs this data from outside in order to process it further and store. In the model it is represented as a separate Stage (see Figure 7). After the information was extracted and hashed it is sent to blockchain. The smart contract that receives the information on the blockchain is represented as separate Stage "Invoice data entering". The connection between stages is represented by sentry connections. Before information being sent to blockchain, firstly, the certificate status is checked by means of tokens for being active that means the company has a valid certificate. In case the company's certificate is suspended and it tries to enter the invoice to the system, the event raises to inform Nepcon and the process is blocked. Some connections on Figure 7 are not complete due to this figure being a part of the full solution represented in Figure 6.

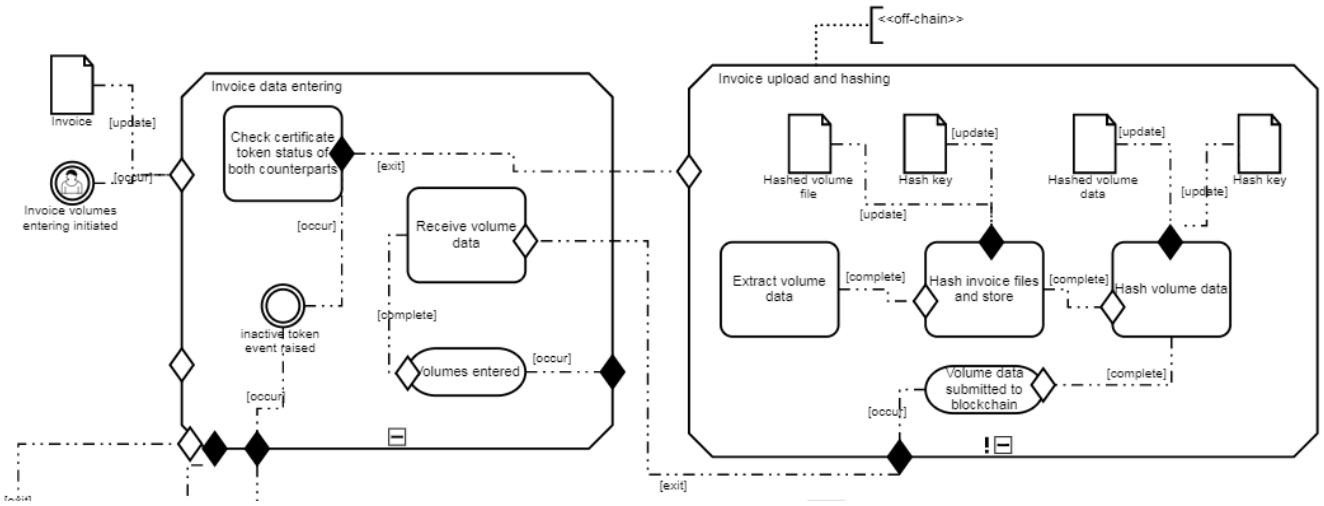

Figure 7. Entering invoice data as Verifier pattern modeled with CMMN

It is possible to model these two Stages as one with the Invoice upload and hashing as an embedded Stage (see Figure 8). However, in this case in one Stage there will be tasks that are included to a Verifier and in a blockchain. For example, as it was said the invoice upload and hashing is a Verifier when the task of checking certificate token status of both counterparts is done within the blockchain system. With the embedded Stage there is no clear distinction between them. It can be done by annotations, however, it was decided to use two separate Stages for better understanding where the task is done.

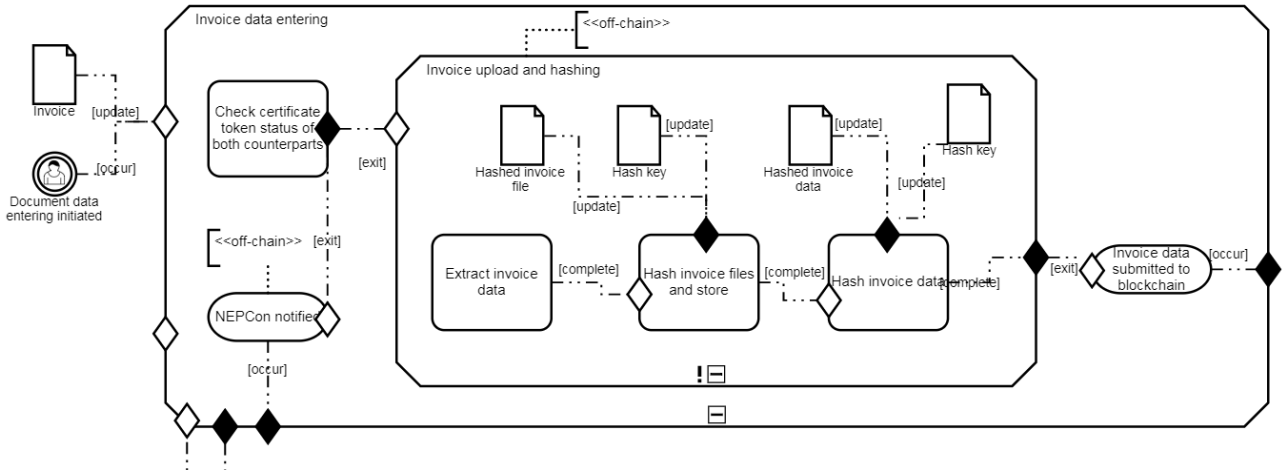

Figure 8. Entering invoice data as Verifier pattern modeled with CMMN (alternative)

The same pattern applies for entering the certificate status to the smart contract by Nepcon (see Figure 9). Based on this information from external party blockchain checks the certificate status of the users to give the access for entering invoices in the system that is represented as a “Check certificate token status of both counterparts” represented on Figure 7. In the model it is shown as a Stage off-chain “Inspection” with a task related to submission the certificate status by a person (Human task) and is further sent to the blockchain system “Token Management”. Later on the certificate token statuses uploaded by Nepcon are checked in Figure 7 while entering the invoice to the system.

How exactly the certificate status is sent to the blockchain system is not represented as it may be done in different ways, for example, using an Oracle to provide the message exchange or the certificate status will be entered directly on blockchain using the analytical node where the information will be further transferred to all other nodes. A task and a milestone are used to show that certificate status is sent off-chain and then is received on-chain with the association between the stages (see Figure 9). For purpose of clarifying the application of Verifier pattern the part of the full solution is presented below.

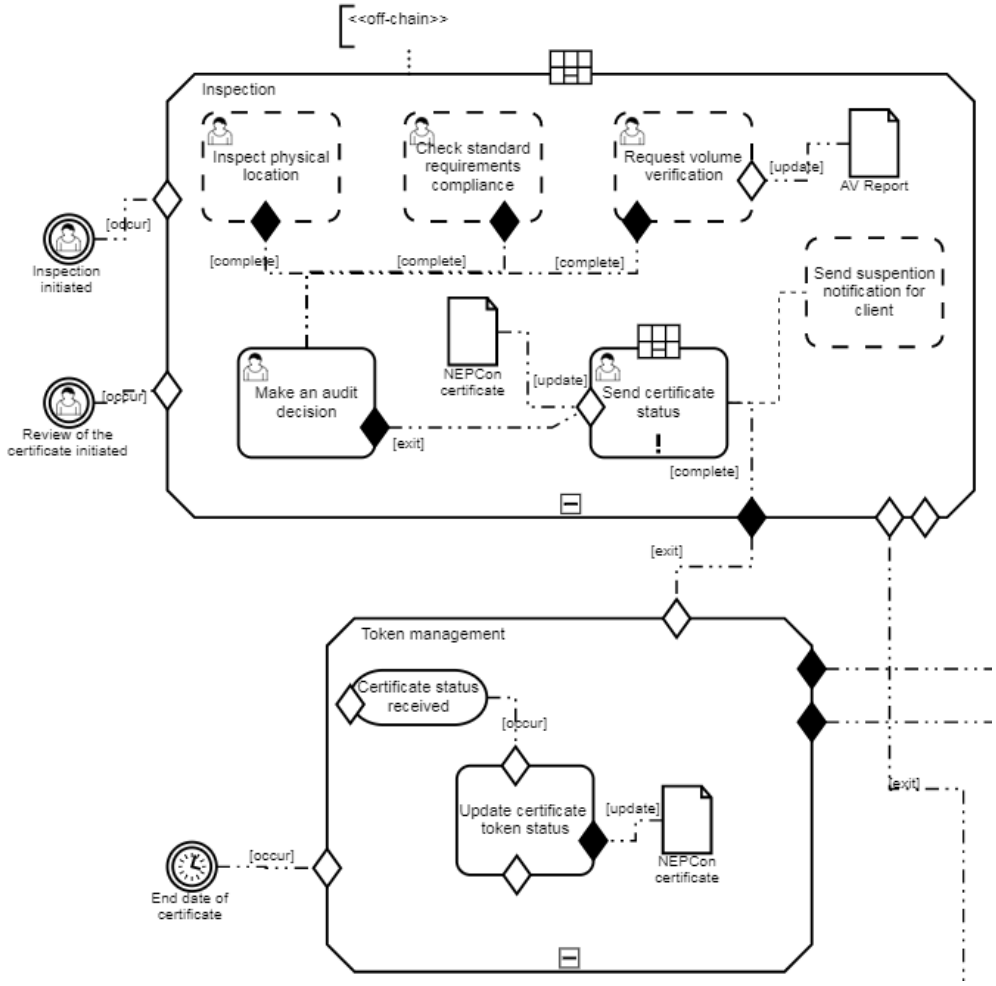

Figure 9. Sending the certificate status into the blockchain system as a Verifier pattern modeled with CMMN

As a Reverse Verifier in the case study there is an analytical verification calculation that are further shown in a Monitor. Monitor is an external information system aimed to provide Nepcon with results of calculations for further investigation of the situation and notify in case of founded mis-conformances (see Figure 10). For these calculations based on a business rule the information stored on blockchain is needed that is why it is a Reverse Verifier. It was decided to put the computations on the analytical node inside blockchain, so that calculations are processed only on one node and then the results are populated within the network. To explicitly state that this process is done on a certain analytical node the annotation with a stereotype was used.

Another example of Reverse Verifier is the notification of Nepcon after the analytical verification that is represented on Figure 10 as a Stage “Monitor” with annotation that this is done off-chain. Entry sentries are connected with Stages (see Figure 6) where the mis-conformances may occur: “Conversion rate change”, “Invoice data entering” and “Analytical verification”. In CMMN the notification of Nepcon can be modelled as a Milestone that comes after the event was raised. The business rule written in a smart contract based on which the suspicious activity is identified is written in the annotation to the task related to verification of volumes for mis-conformances. On Figure 10 the part of the full solution is presented where the aggregation calculations are done and are transferred to Monitor so that Nepcon could see the results or notifications of potential fraud.

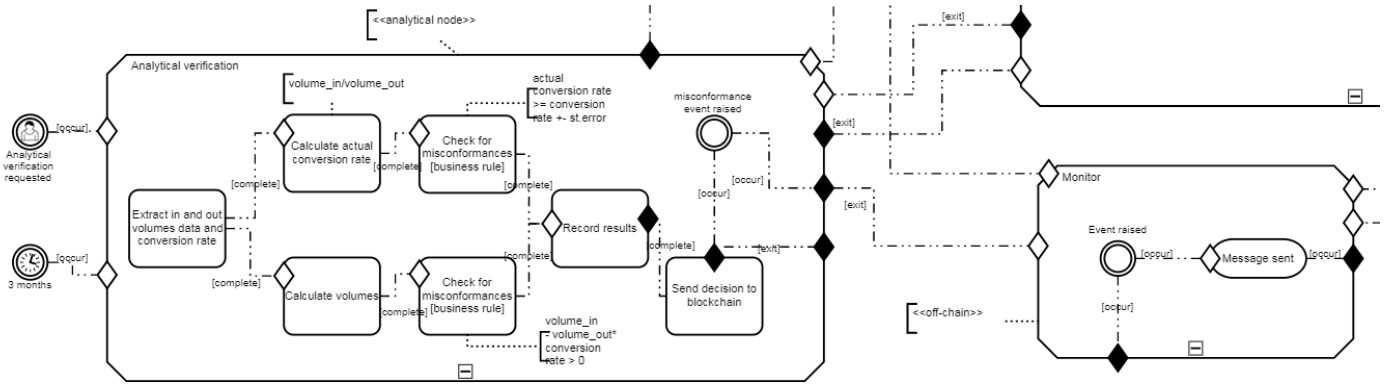

Figure 10. Sending the results after the analytical verification from blockchain as a Reverse Verifier pattern modeled with CMMN.

Another pattern in this group *legal and smart contract pair* (pattern 3) concerns the link between the physical agreement and digital representation of it by a smart contract. Digitalization of the legal industry is increasing within last years. For example, usage of digital signature is already a valid way to sigh the legal agreements. Blockchain can be a platform that is trustworthy to execute the legal agreements as on-chain smart contracts.

In our case there are no digital legal agreements in place, however, physical legal agreements between Nepcon and companies exist. The companies should sign a legal agreement with Nepcon so that Nepcon can have access to the internal data to conduct the inspections and also can add a company into the system as a user. There are also legal limitations for the operations of the company that Nepcon checks during the inspection such as the company can sell products as certified only if it has a certificate for this specific product, the company cannot sell more that it buys (conversion rate), working conditions should comply with existing standards for the industry etc. According to those agreements and standards Nepcon conducts inspections and in case of revealing the mis-conformances can suspend the certificate.

In the model the initial process of agreement is represented in an onboarding process on Figure 5 where the certificate issued by Nepcon is mirrored on blockchain. The process of entering the certificate status that takes place after initial audit is represented by the task of issuing the certificate token with associated Data Object – Certificate from Nepcon. During the next audits Nepcon inserts a certificate status after making a decision according to inspection results (see Figure 9).

The representation of legal agreement conditions is also represented by a trigger that occurs to notify Nepcon about suspicious activity after the analytical verification. This is represented by an event listener “Misconformance event raised” in Analytical verification and “Event raised” in Monitor that are connected with sentries (see Figure 10). After the examination of the situation Nepcon can suspend the certificate manually by changing the status of the certificate that is further registered on blockchain in “Token management”. This is captured by the task of submission the certificate status that will further change the certificate token status (see Figure 9).

One more example of legal agreement conditions is the changes of the certificate status when the certificate expires. As it was said after certificate status being changed to “suspended” the

company cannot anymore access the system to upload the invoices. On Figure 9 the Timer Event Listener triggers the task of changing certificate token status in Token Management.

However, it should be notices that for now there are no regulatory base now for the smart contracts. As well blockchain is not yet mature to provide the legal restrictions for the operations.

4.3. Patterns for Data Management

Patterns for data management includes *encrypting on-chain data* (pattern 4), *tokenization* (pattern 5), *off-chain data storage* (pattern 6), and *state channel* (pattern 7).

For the businesses there is a need to protect their commercially crucial data. It may be, for example, the prices for customers as they may be different for different clients or sales volumes. Such information should be accessible only for selected participants or only for internal usage. The main problem is that all information within the network is accessible by all participants that of course ensure transparency. For ensuring the confidentiality the *encryption of certain data* (pattern 4) should take place before entering the information into blockchain. This implies generation of public and secret key off-chain to ensure that only participants with secret key can decrypt the data. With this a drawback of security comes up. As key management is done off-chain there is a risk of sharing the key that gives access to all the internal information.

In our case, it is vital for the business to protect their internal information as confidentiality of their transactions thus commerce operations are a crucial factor to join the blockchain system. It is obvious that this pattern should be in introduced in the system, however, in the standard specification of CMMN there is no way to model the process of encrypting the data. Not only the process of encryption is an obstacle, but also a difference between the encrypted and not-encrypted data that is not provided by CMMN. With encryption also key generation and key management should be modelled. The process of key generation can be depicted as a task with associated data object – key (see Figure 7). However, it is necessary to show the difference between the public and secret key.

This is more technical requirement for the system that is not captured by the notation because of its orientation to business processes. A way for solving this problem can be adding a specific sign to the tasks that will show where the data is encrypted [60]. Another possibility is to have annotation to every data object and task related to data entering. However, if there are a lot of documents and such task in the model, it will be filled with annotation, so the special signs are preferred.

Tokenization (pattern 5) refers to the usage of tokens on a blockchain. Tokens represent the physical goods in the digital world. Blockchain platform can be used to implement the tokenization in a way that tokens represent monetary value or other physical assets. For now, this is done by naïve tokens, for example, BTC on Bitcoin. Better way to realize tokenization is to use smart contracts to represent physical assets.

For Nepcon case a traded goods could be represented as a token. That would be useful to track the product through all the stages of production to ensure the provenance. However, in or case in the charcoal production the good is changing its form from round wood into charcoal, that makes it impossible to track it. Another good that can be represented as a token is the certificate issued by Nepcon. The certificate has a unique id, status (active/suspended) that can be changed manually, for

example, in case of revealing mis-conformances that lead to suspension or automatically on the end date of certificate validity. The way to introduce token is to generate it after the contract with Nepcon is signed. Along with entering the certificate in the system, the company will be added in the system as a user and the token for the certificate will be generated. Every time the participant needs to enter the data the token status will be checked.

During the onboarding process once Nepcon enters the certificate status is sent to blockchain, the Registration of the certificate stage starts (see Figure 5). This implies issuing the token for the certificate with an active status. Tokenization in an auditing process is modeled as a separate stage. This task represents changing of the status of the token as later the certificate status can be changed either because of expiration, either because Nepcon can make a change. To change the certificate status Nepcon should investigate the situation or conduct additional audit that is represented by "Inspection" stage on a Figure 9. For example, after the inspection the certificate can be suspended because of mis-conformances a company has or vice versa after additional inspection all mis-conformances were eliminated, so the certificate will be again active. In the model the changing of its status is represented by a task "Update certificate token status" that can be executed after receiving the status of certificate (see Figure 11). The task is associated with the Data Object – Nepcon Certificate. The connection between inspection stage and token management stage is an exit – entry sentry-based connection. The propagation of the decision, by means of cryptographic protocol, would be possible to be modeled with annotations but CMMN does not allow annotation on connectors. The part of the model is used to explain Tokenization patterns modeled with CMMN.

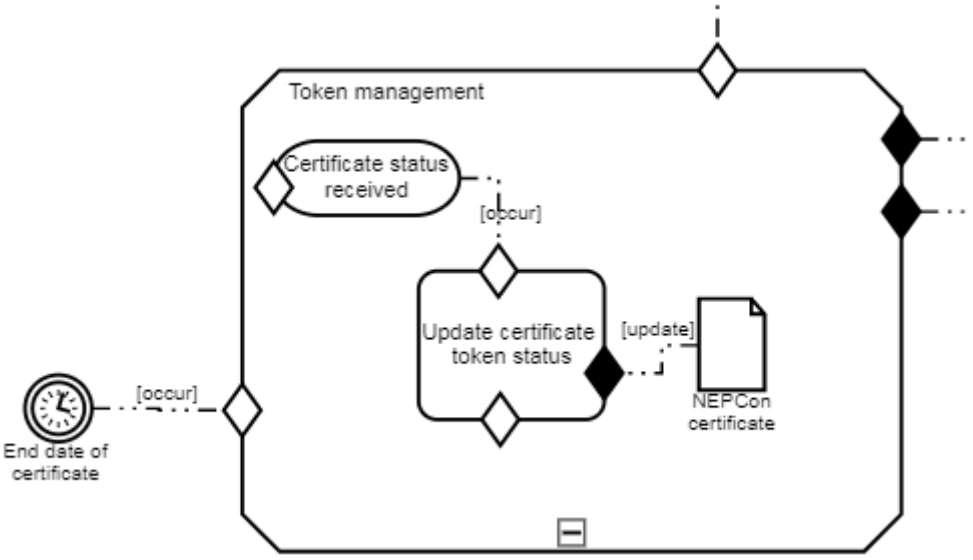

Figure 11. The process of token management as Tokenisation pattern modeled with CMMN

There is also a connection with another stage – Invoice Data Entering where the verification of the token status is needed for giving the right to insert the information about transaction (see Figure 7).

Speaking about *off-chain data storage* (pattern 6) it should be mentioned that blockchain has a limited capacity for storing the information due to the block sizes and number of blocks. However, there is no guarantee that the data being stored off-chain can be immutable. To solve this problem the hashing of the information was proposed in order to store the representation of the data that will have

smaller size. The hashing process in essential to ensure the traceability between off-chain data and the information stored on-chain.

In the case study there is a document flow between participants that is needed to be captured as the information from them is analyzed. Digital version of the documents is a pdf file that is not reasonable to store on-chain. However, storing the information outside is risky for the business. That is why it is preferable to store the documents outside blockchain with the extracted and hashed data on-chain for further analysis. This will allow to have lower storage usage and in case the real documents are needed (to check for mis-conformances) they can be found using hash as a reference from summary on chain to the pdf document. There are two options how to do that. One option is manual. So that the company uploads the document and enters manually the needed information from the document. This option will bring manual errors and room for playing around the figures that may be explained as manual error. More secure option is to have in place an information system that will extract the needed data from the document automatically. It was discussed that this system should be run outside blockchain with only transferring the summary data and hash to the blockchain system. This brings another concern about trustworthiness of the software as it will hash the information.

The differentiation of on-chain and off-chain data to show the internal and external storages is not supported in CMMN as there is no specific object in the notation for the databases. In the model each stage is used to show the process done in one specific system thus it is possible to use different colors for the stages in order to show what is done off-chain or on-chain and thus is saved in different databases. Another option is to add a stereotype as an annotation (for example, <<off-chain>>) to the stages to explicitly state which processes are taken place off or on-chain (see Figure 6). In the modeling software used for this case study - Camunda [61] it is not possible to add another line below the stage name that is why the stereotype is added as an annotation.

The hashing process for off-chain data is needed to ensure consistency that is another challenge for CMMN to show this process and hashed data in the model. Currently this important process of blockchain is not supported by CMMN. In this case study the hashing process is captures as a separate off-chain stage where the tasks related to hashing are performed. Additionally, the Data Objects were used to show the associated hashed documents along with the generated hash key for them. In the notation there are no elements that could be used to distinguish between different types of data such as encrypted, hashed or on-chain. For now, it is not possible to show this as the notation was not designed for such technical issues. In the model it was done by using annotations. However, the better way is to have a specific sign for the tasks and data objects.

The *state channel* (pattern 7) in the paper [20] is focused on the micro-payments transactions and it is suggested to perform transactions off-chain and periodically record a set of micro-transactions on-chain.

In the context of the case study there are no payments in the model. However, as a representation of this pattern the inspection process can be used. During the inspection there are several steps: physical inspection, verification of a list of standards, review of the report, etc. In order not to enter each of those steps on blockchain only the final decision about the certificate will be entered that is an aggregated decision from a micro-decision during the inspection process.

In the CMMN is represented as two stages: Inspection that is a process outside of blockchain where all the micro-decisions are made and “Token management” that is done on-chain where the decision of inspection is recorded (see Figure 9). The set of micro-decisions can be shown as a set of

tasks. The final decision can be finished and thus transferred on blockchain only when all micro-decisions - tasks are finished. This is represented by an Entry Sentry that wait for the completing of all associated tasks on a Figure 12. As the inspection process can consists of different steps according the type of inspection (first inspection or additional to check the company's performance according to the specific notifications received from blockchain) the tasks are Discretionary Tasks and are synchronized in the task "Make a decision". If the set of tasks are predefined in advance and are represented by simple Tasks, then the associations will be synchronized in the Entry Sentry of the task "Make a decision". The connection between stages can be represented only with sentry connectors where it is not possible to specify the type of connector being of state channel. The only option to clarify it is to use annotations that is not possible with connectors.

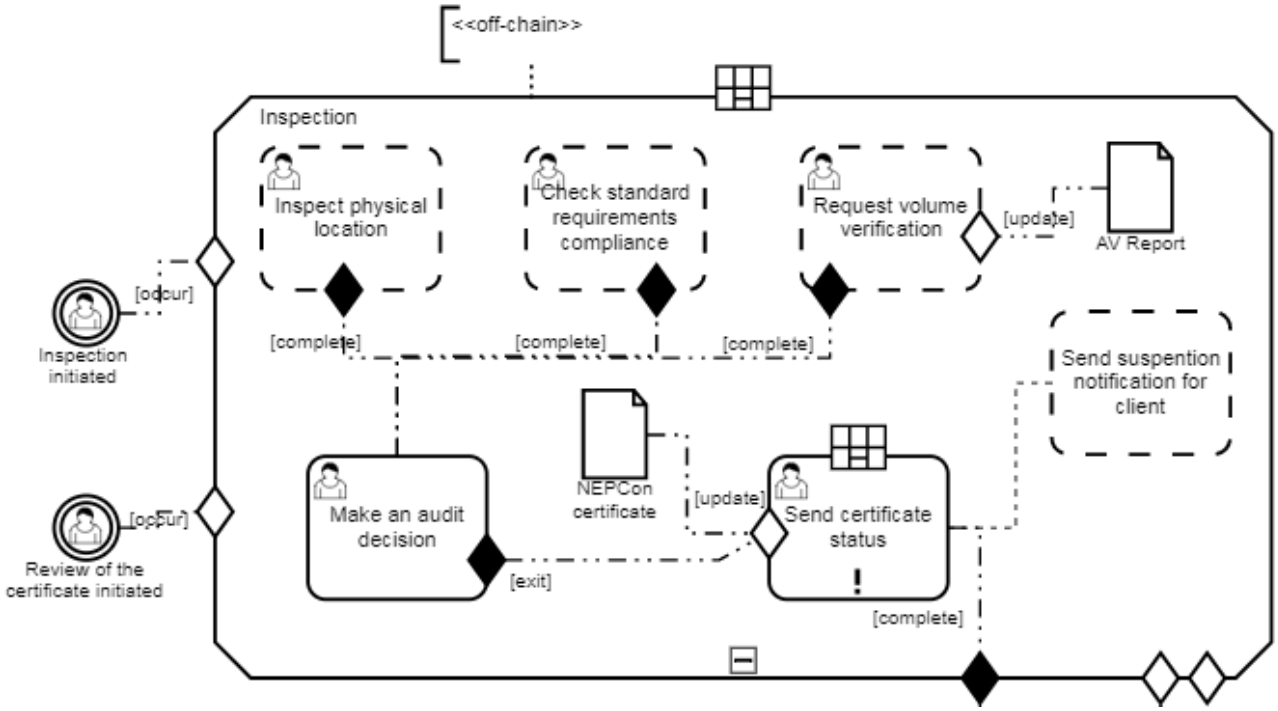

Figure 12. The process of inspection as State Channel pattern modeled with CMMN

4.4. Patterns for Security

Security patterns cover aspects that deal with *multiple authorization* (pattern 8), *off-chain secret enabled dynamic authorization* (pattern 9), and *x-confirmation* (pattern 10).

Some transactions cannot be recorded before several authorities didn't approve it, for example, payments transactions. It means that *multiple authorization* (pattern 8) is needed.

In the case study there is a case where approval from another party is necessary to record the transaction. This happens when a company enters new conversion rate that cannot be updated automatically, so Nepcon should review it and approve. Thus, the transaction will have two parties involved – company who enters a conversion rate and Nepcon.

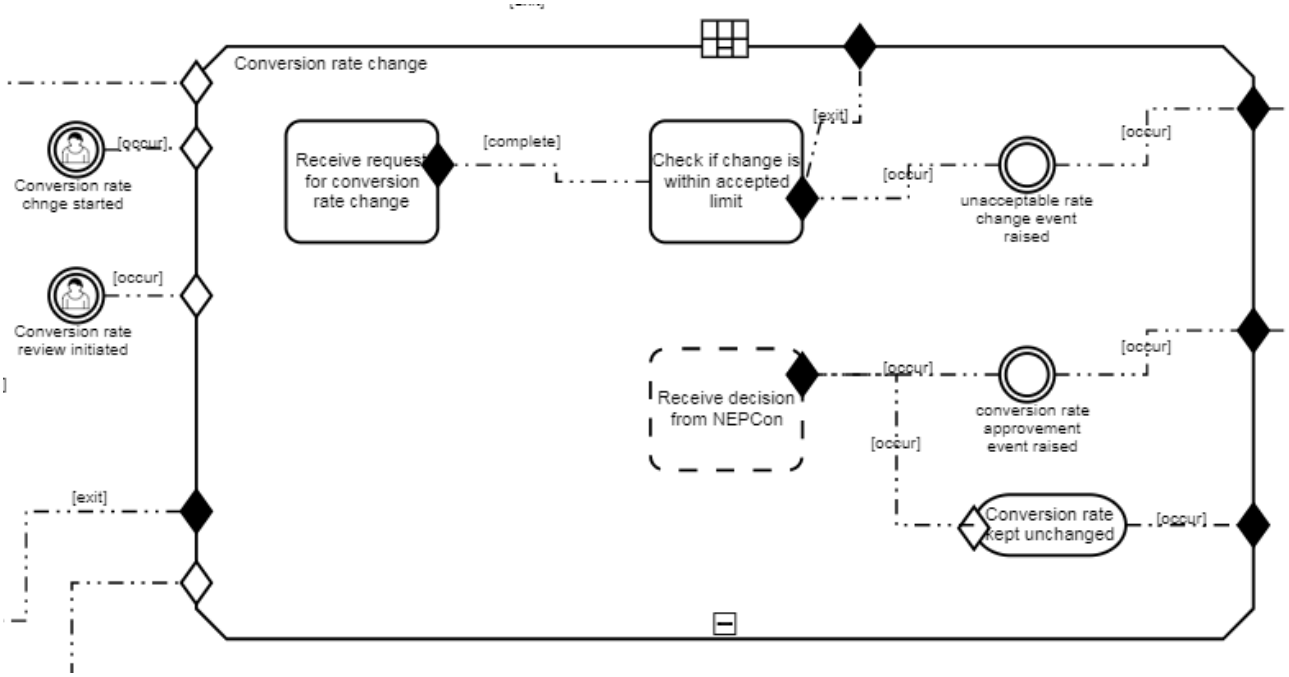

Figure 13. The process of conversion rate change as Multiple Authorization pattern modeled with CMMN

On Figure 13 conversion rate update is represented as a separate stage being a part of a full solution on Figure 6. The case of multiple authorization is represented by tasks that are needed to record the transaction. So, firstly, the company enters the new conversion rate, however, it will not be updated until Nepcon approves it. It means, that another party – Nepcon should review the conversion rate and make a decision. That is why in this stage there is a discretionary task performed by Nepcon "Review new conversion rate" and is represented by blocking human task. When a company wants to update their conversion rate the Monitor will react on a raised event on the blockchain and will notify Nepcon which is represented by exit-entry sentries connection (see Figure 6). In our case there are no documents that should be sign as it is assumed in the pattern, but the modeling of the signature is the same as just having the approval from Nepcon.

In case there are more parties needed to approve the transaction, it can be specified in the Properties Panel where the Performers can be specified (Candidate Users). Camunda extensions also allow to specify the performers that are unknown at the design time or they depend on the data. For such cases assignment expressions are used [62]. As in our case we have only the approval from Nepcon the annotation was used for easier understanding of the model. In case when parties should approve the transaction, the set of tasks can be modelled with the synchronization in the Entry Sentry of another task or a milestone.

The *Off-Chain Secret Enabled Dynamic Authorization* (pattern 9) is related to the transaction authorization by the unknown parties during the first transaction submission. However, this may happen only in the public blockchain systems. In our case there is a private blockchain system where all participants are known. However, it is possible to model this case with a Task of generation special file with a key (Data Object) that is transferred to the parties who should approve the transaction. Before approval of the transaction the task with verifying the key can be added.

In blockchain there is a chance that recently added few blocks are replaced by a competing chain fork. The security strategy is to wait for the certain number of blocks (X) to be generated and then include the transaction into the block. This is an *x-confirmation* (pattern 10).

As this is very technical issue that is not supported by the modelling notation it is out of scope of this study. However, in CMMN there are two ways of modelling this situation. Firstly, it is possible to add the condition to the Entry Sentry of the task that execute adding transaction to the block. Another way is to add the Repetition Rule to the Task or Stage where the transactions are added to the block to specify when the Task or Stage will be executed.

The first research question addresses the applicability of the notation for blockchain-oriented solutions. It was found that CMMN can be used to adequately represent processes based on blockchain system. For modeling such a process one case plan is used where sub-processes executed in different systems can be shown in Stages. To distinguish the difference between blockchain and external systems the annotations are used. Smart contracts are also modeled as Stages. For notifying Nepcon i.e. communication between blockchain and external system the event listeners with another Stage are used as blockchain system does not support message flows. When the event is raised the Monitor, being an external system, will send a notification that is modeled as a Milestone. To represent activities executed on blockchain system such as encryption of data tasks are used along with annotated data objects to specify the data type.

4.5. Suitability of CMMN

The design patterns for blockchain-based applications were used for the analysis of the strengths and weaknesses of the CMMN in regard to modeling blockchain-oriented processes that is a second research question. In this section the summary of the findings is presented.

In CMMN it is possible to model the whole solution in one Case Plan Model that is an advantage for understanding of the whole process. According to the analysis some of the patterns are supported by CMMN without additional explanation that makes this notation suitable for modeling blockchain-based solutions. However, there are important aspects related to blockchain technology that are not easily captured by CMMN like hashing or encryption of data, on-chain and off-chain data storage and a concept of smart contract. Some of the elements are not currently presented in CMMN that is why there is a need to use annotations to clearly present them on a model. Furthermore, these elements are crucial for blockchain solutions and commonly occurring according to the pattern collection. The first thing that is not possible to model in this notation is where the process is executed within the blockchain-based system (on-chain) or is executed externally (of-chain). In CMMN the case plan is self-contained where each stage represents a part of a case (sub-process). Sub-processes executed on-chain like smart contracts are represented alongside off-chain sub-processes, for instance, Monitor. The distinction between them can be done only by the usage of annotations with stereotypes attached to the stages. This applies also to the distinction between data storages (pattern 6). With the annotation of the stages, the data within a stage (case file items) are assumed to be stored within the same system. However, with CMMN it is possible to model different systems within one stage i.e. one case file item may be stored externally whereas another one on-chain. To clearly distinguish where the data is stored the annotations to the case file items are used.

Another important aspect within blockchain technology are encryption and hashing of data that should be represented on conceptual models of blockchain-based business processes. With CMMN such distinction of hashed and not hashed data or encrypted and not encrypted data can be made only by means of annotations on the level of case file item. In order not to use annotations as in complex business processes the model may be overwhelmed with them the additional extensions are proposed. For better distinguishing of the data type (encrypted, hashed, etc.) a special data element is needed. It is also important to understand where the data is stored. Therefore, a special element for specifying on-chain and off-chain data is required. Such special elements may be presented by a new data type in notation or by a decorator for a current case file item. One more marker is needed for stages to clearly represent whether a sub-process is a smart contract or not. As a concept of tokens is important for blockchain-oriented solutions it should be separated from other elements. Currently, tokens are represented by stages as all other sub-processes including smart contracts. For this purpose, a new element type is proposed to be added in notation.

All current limitations of CMMN for representing blockchain components with proposed extensions are shown in Table 2.

Table 2. Proposed solutions for current limitations

Blockchain component	Current solution	Proposed solution
Smart contract	Stage as all other sub-processes	A marker denoting that a sub-process/stage is a smart contract
Hashed data	Annotation on the level of case file item	A new type of data object that represents hashed data
Encrypted data	Annotation on the level of case file item	A new type of data object that represents encrypted data
On-chain/Off-chain data storage	Annotation with stereotype on the level of stage	A marker denoting if the data is stored on- or off-chain
Token	Stage as all other sub-processes	A new element type representing tokens

Thus, answering the second research question about strengths and weaknesses of the CMMN in regard to modelling blockchain-based solutions it should be said that CMMN can represent blockchain-oriented processes, however, it requires additional elements for existing notation to capture the important technical details of blockchain solution. As it is now, the CMMN weaknesses are addressed by annotations either on the level of stage, either on the level of case file item.

4.6. Threats to Validity

Case studies have threats to validity that should be considered. Such threats include external validity and reliability [63].

The results of a case study are considered within a specific context – setting of a case study. However, the question of generalizing the findings beyond this context is meant by external validity. The models depend on the information from domain experts, the purpose of the study and a modeler's

competence. That is why CMMN models could be done in a different way having different use case, for example. It should be also mentioned that the models were discussed with two other experts and the notation of CMMN was followed to the extent possible given that CMMN does not fully serve blockchain-oriented processes.

The dependency between the results and the modeler is addressed by a reliability threat that implies the question whether the models would look the same if the research was conducted by different person. This threat was partially tackled by verifications of the models with domain experts and peer debriefing [64]. Data triangulation (usage of documentation and information from domain experts) was used to ensure better reliability. Moreover, observer triangulation was used also as a group of researchers was working on this case study and participated in the interviews: my supervisors, I and another master student who was working on the same case study with different modeling notation. To avoid biases and guarantee the independence of our research studies no particular notation was used during the interviews and there was no exchange of results.

5. Conclusions

This paper has as purpose to analyze the suitability of CMMN for modeling processes running on blockchain. In order to address the research questions the case study of auditing process in a timber-to-charcoal process was conducted. As a basis for the analysis a set of patterns for blockchain-based applications was used.

It was found that CMMN can be used to model blockchain-oriented processes and can adequately represent commonly occurred patterns for blockchain-based application. Existing elements of the notation can be used to model blockchain-based solution, however, to clearly represent the process with important technical details of blockchain technology like difference between on-chain and off-chain data storage or encryption of data there is a need to use annotations. For better suitability of CMMN for such technical aspects the extensions were proposed.

The extensions address the issues of distinguishing the data storages between on-chain versus off-chain and between data type like hashed or encrypted data. Additional extensions for separating smart contracts and tokens from other the sub-processes are suggested.

The findings in this paper are limited to a case study research i.e. they have a limitation in the extent they can be generalized. However, the main results can be useful for process analysts in deciding to use CMMN or not for redesign the processes running on a blockchain solution and if so, how to use this notation.

In this paper, the focus was on an artefact-centric modeling language for representing blockchain-oriented processes. It should be mentioned that understandability of the models was not considered. That is why, further investigations in empirical evaluation and analysis of artefact-centric approach are needed.

References

1. Timothy B. Lee. Five years of Bitcoin in one post. The Washington Post. 2014.
2. Evans, D. S. Economic aspects of Bitcoin and other decentralized public-ledger currency platforms. *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, 2014. No 685. p. 14.
3. Borenstein J. A Risk- Based View of Why Banks Are Experimenting with Bitcoin and the Blockchain: 2015. http://www.risktech-forum.com/opinion/a-risk-based-view-of-why-banks-are-experimenting-with-bitcoin-and-the-block. (20.03 2019)
4. Belinky, M., Rennick, E., & Veitch, A. The fintech 2.0 paper: Rebooting financial services. *Oliver Wyman, Anthemis Group and Santander Innoventures*, 2015. *http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf*
5. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2016, No 2(6-10), 71.
6. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. Blockchain contract: Securing a blockchain applied to smart contracts. *IEEE international conference on consumer electronics (ICCE)*, 2016. pp. 467-468.
7. Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. Blockchain–the gateway to trust-free cryptographic transactions. Berlin, Heidelberg: Springer. 2016.
8. Davenport, T. H., & Short, J. E. The new industrial engineering: information technology and business process redesign. 1990.
9. Van Der Aalst, W. Process mining: discovery, conformance and enhancement of business processes (Vol. 2). Heidelberg: Springer. 2011.
10. Dumas, M., La Rosa, M., Mendling, J., Reijers, H. Fundamentals of Business Process Management. Berlin, Heidelberg: Springer. 2013.
11. Dumas, M., van der Aalst, W., & Ter Hofstede, A. (Eds.). Process aware information systems (Vol. 1). Chichester: Wiley. 2005.
12. Davenport, T.H., Short, J.E.: The New Industrial Engineering: Information Technology and Business Process Redesign. *Sloan Management Review 31*, 1990. pp. 11–27.
13. Object Managment Group (OMG): Business Process Model and Notation (BPMN) Version 2.0. 2011.
14. Object Managment Group (OMG): Case Management Model and Notation (CMMN) Version 1.1. 2016.
15. Cohn, D., & Hull, R. Business artifacts: A data-centric approach to modeling business operations and processes. *IEEE Data Eng. Bull*. 2009. 32(3), pp. 3-9.
16. Hull, R., Batra, V. S., Chen, Y. M., Deutsch, A., Heath III, F. F. T., & Vianu, V. Towards a shared ledger business collaboration language based on data-aware processes. *International Conference on Service-Oriented Computing*. Springer, Cham. 2016, pp. 18-36.
17. Hull, R., Llirbat, F., Siman, E., Su, J., Dong, G., Kumar, B., & Zhou, G. Declarative workflows that support easy modification and dynamic browsing. *ACM SIGSOFT Software Engineering Notes*, 1999, *24*(2), pp. 69-78.
18. Falazi, G., Hahn, M., Breitenbücher, U., & Leymann, F. Modeling and execution of blockchain-aware business processes. *SICS Software-Intensive Cyber-Physical Systems*, 2019, *34*(2-3), pp. 105-116.
19. López-Pintado, O., García-Bañuelos, L., Dumas, M., & Weber, I. Caterpillar: A Blockchain-Based Business Process Management System. *BPM (Demos)*. 2017.

20. Xu, X., Pautasso, C., Zhu, L., Lu, Q., & Weber, I. A pattern collection for blockchain-based applications. *Proceedings of the 23rd European Conference on Pattern Languages of Programs*. New York: ACM. 2018. pp. 3-20.
21. Lavanya, B. M. Blockchain Technology Beyond Bitcoin: An Overview. *International Journal of Computer Science and Mobile Applications* 6.1, 2018. pp. 76-80.
22. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE. 2017. pp. 557-564.
23. Lamport L., Shostak R. & Pease M. The byzantine generals problem, ACM Transactions on Programming Languages and Systems (TOPLAS), 1982. vol. 4, no. 3, pp. 382–401.
24. Nakamoto S., Bitcoin: A peer-to-peer electronic cash system, 2008. https://bitcoin.org/bitcoin.pdf
25. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 2018, pp. 352-375.
26. Christidis K., Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. *2016 IEEE The Plethora of Research in Internet of Things (IoT)*, IEEE. 2016, pp. 2292 - 2303.
27. Bartoletti M., Pompianu L. An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns. *International Conference on Financial Cryptography and Data Security*. 2017, pp. 494–509.
28. Zhang K., Jacobsen H.A. Towards dependable, scalable, and pervasive distributed ledgers with blockchains. *International Conference on Distributed Computing Systems*. 2018, pp. 1337–1346.
29. Ethereum Official Website. https://www.ethereum.org/
30. Buterin, V. A next-generation smart contract and decentralized application platform. *white paper*, 2014, *3*, 37.
31. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. The blockchain as a software connector. *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, IEEE. 2016, pp. 182-191.
32. Konstantinidis I., Siaminos G., Timplalexis C., Zervas P., Peristeras V., Decker S. Blockchain for Business Applications: A Systematic Literature Review. *Business Information Systems*, 2018, pp.384-399.
33. Hou, H. The application of blockchain technology in E-government in China. *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, IEEE. 2017, pp. 1-4.
34. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. How blockchain could empower ehealth: An application for radiation oncology. *VLDB Workshop on Data Management and Analytics for Medicine and Healthcare*, Cham: Springer. 2017, pp. 3-6.
35. Münsing, E., Mather, J., & Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. *2017 IEEE conference on control technology and applications (CCTA)*, IEEE. 2017, pp. 2164-2171.
36. Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access*, *5*. 2017, pp. 17465-17477.
37. Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, 2016, *2*(1).
38. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 2018, *7*(4), pp. 6-14.
39. R3 Official Website. https://www.r3.com/

40. Li, W., Sforzin, A., Fedorov, S., & Karame, G. O. Towards scalable and private industrial blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, ACM. 2017, pp. 9-14.
41. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Song, D. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg: Springer. 2016, pp. 106-125.
42. Kosba, A., Miller, A., Shi, E., Wen, Z. & Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, *Proceedings of IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 839–858.
43. Hyperledger Official Website. http://www.hyperledger.org.
44. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, ACM. 2018, pp. 30-35.
45. Cachin, C. Architecture of the hyperledger blockchain fabric. *Workshop on distributed cryptocurrencies and consensus ledgers* 2016, Vol. 310.
46. Kosba, A., Miller, A., Shi, E., Wen, Z. & Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, *Proceedings of IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 839–858.
47. Van der Aalst, W. M., Weske, M., & Grünbauer, D. Case handling: a new paradigm for business process support. *Data & Knowledge Engineering*, 2005, *53*(2), pp. 129-162.
48. Grudzińska-Kuna, A. Supporting knowledge workers: case management model and notation (CMMN). *Information Systems in Management*, 2013, *2*.
49. Breitenmoser, R., & Keller, T. Case management model and notation-a showcase. *European Scientific Journal*, 2015, *11*(25).
50. Robson, C. Real world research 2nd edition. *Malden: BLACKWELL Publishing*. 2002.
51. Andersson, C., & Runeson, P. A spiral process model for case studies on software quality monitoring—method and metrics. *Software Process: Improvement and Practice*, 2007. *12*(2), pp. 125-140.
52. Stake, R. E. The art of case study research. Sage. 1995.
53. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B., & Wesslén, A. Introduction to Experimentation in Software Engineering. 2000.
54. Kitchenham, B. A., Pfleeger, S. L., Pickard, L. M., Jones, P. W., Hoaglin, D. C., El Emam, K., & Rosenberg, J. Preliminary guidelines for empirical research in software engineering. *IEEE Transactions on software engineering*, 2002, *28*(8), pp. 721-734.
55. NEPCon Official Website. https://www.nepcon.org/
56. Assurance services international Official Website. www.asi-assurance.org
57. Francisco, K., & Swanson, D. The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2018, *2*(1), 2.
58. Korpela, K., Hallikas, J., & Dahlberg, T. Digital supply chain transformation toward blockchain integration. *Proceedings of the 50th Hawaii international conference on system sciences*. 2017.
59. Gamma, E. Design patterns: elements of reusable object-oriented software. *Pearson Education India*. 1995.
60. Rodríguez, A., Fernández-Medina, E., & Piattini, M. A BPMN extension for the modeling of security requirements in business processes. *IEICE transactions on information and systems*, 2007, *90*(4), pp. 745-752.
61. Camunda Official Website. https://camunda.com
62. CMMN Manual: User Tasks. Camunda Website. https://docs.camunda.org/manual/7.8/reference/bpmn20/tasks/user-task/#assignment-based-on-data-and-service-logic

63. Runeson, P., & Höst, M. Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering*, 2009, *14*(2), pp. 131-164.
64. Runeson, P., Host, M., Rainer, A., & Regnell, B. Case study research in software engineering: Guidelines and examples. John Wiley & Sons. 2012.

Appendix

License

Non-exclusive licence to reproduce thesis and make thesis public

I, Svitlana Filipova,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

Modeling Business Processes on a Blockchain Ecosystem using CMMN,

supervised by Fredrik Milani and Luciano García-Bañuelos.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Svitlana Filipova

10/08/2019