Automatic smart contract generation using controlled natural language and template

T. Tateishi
S. Yoshihama
N. Sato
S. Saito

Smart contracts, which are widely recognized as key components of blockchain technology, enable automatic execution of agreements. Since each smart contract is a computer program that autonomously runs on a blockchain platform, their development requires much effort and care compared with the development of more common programs. In this paper, we propose a technique to automatically generate a smart contract from a human-understandable contract document that is created using a document template and a controlled natural language (CNL). The automation is based on a mapping from the document template and the CNL to a formal model that can define the terms and conditions in a contract including temporal constraints and procedures. The formal model is then translated into an executable smart contract. We implemented a toolchain that generates smart contracts of Hyperledger Fabric from template-based contract documents via a formal model. We then evaluated the feasibility of our approach through case studies of two types of real-world contracts in different domains.

1 Introduction

Smart contracts are computer programs that run on blockchain platforms and execute a variety of commercial agreements such as financial contracts and purchase agreements. From the engineering perspective, the terms and conditions of each legal contract are equivalent to the software requirements that the program should satisfy. Therefore, engineers who work on a smart contract must understand the contents of the contract and communicate with a business person to elicit and clearly define the software requirements. This task is often error-prone and requires much effort to verify the requirements. There have been many studies on formal models of legal contracts [1] for the sake of verifying the semantic aspect of such contracts. However, it is still difficult to guarantee that the formal models accurately represent the contracts, as the formal models are difficult for business persons or attorneys to understand. In order to mitigate the efforts and the risks of smart contract development, we propose a method for automatically generating smart contracts from legal contract documents.

Considering the structure of commonly used legal contracts, it is reasonable to take a template-based approach to generate smart contracts. For example, in the financial domain, each contract is created based on a master agreement and a term sheet. This structure of the contract is a widespread practice, where the master agreement is a basic agreement between two or more parties that is effective for long periods of time, while the term sheet defines the variable terms and conditions of each contract. Likewise, purchase agreements between two companies often consist of a master agreement and purchase orders, where only the content of the purchase order, such as item names and prices, is varied in each of the agreements. This is because, in many types of contracts, the majority of the logic in each contract is identical, while variable parts are generated from a term sheet. Note that each term sheet (or purchase order) can be regarded as a set of parameters that take not only a simple value such as a number and date, but also various conditions described in natural language. Obviously, the safety of smart contracts is a significant concern among those who aim to use them for commercial purposes. If a smart contract includes vulnerabilities, it can result in huge financial losses, as exemplified in the DAO incident [2]. Therefore, the generated smart contract must never deviate from the expected behavior.

Digital Object Identifier: 10.1147/JRD.2019.2900643

In this paper, we introduce the notion of contract document templates associated with formal models to automatically generate smart contracts. The formal models define the requirements and constraints of a contract in a formal manner. With this approach, we can create more smart contracts with fewer engineers since the generation of smart contracts is fully automated. Given that contract documents are created by business persons or attorneys, only the creation of a template, from which we can automatically generate as many smart contracts as the contract documents, requires an engineer. On the other hand, in a naïve development approach where the development of a smart contract is required for each of the contract documents, we need as many engineers as the contract documents. On the basis of this idea, we implemented a set of tools to generate chaincodes, which are smart contracts of Hyperledger Fabric.[1] We then apply these tools to a purchase agreement and a financial derivative contract.

1.1 Contributions of this paper

The contributions of this paper are as follows.

1) We designed a mechanism to convert a legal contract document into an executable smart contract via a formal model, where the legal contract document consists of a document template and terms and conditions.
2) We provide a set of software tools to automatically generate executable smart contracts from contract documents.
3) We demonstrated the feasibility of our approaches through examples of financial and non-financial agreements.

1.2 Organization of this paper

Section 2 of this paper provides an overview of our approach. Section 3 describes the detailed steps to generate smart contracts. Section 4 describes our implementation. In Section 5, we evaluate the feasibility of smart contract generation through case studies of two types of real-world contracts. Finally, Section 6 summarizes related work, and we conclude in Section 7 with a brief summary.

2 Our approach

Figure 1 outlines our approach of smart contract generation, where the contract document consists of a contract document template and a set of parameter values written in a controlled natural language (CNL). The CNL is a subset of natural language whose grammar is predefined so that a program can understand accurately. The contract

[1]Hyperledger Fabric is a blockchain implementation and one of the Hyperledger projects hosted by The Linux Foundation.

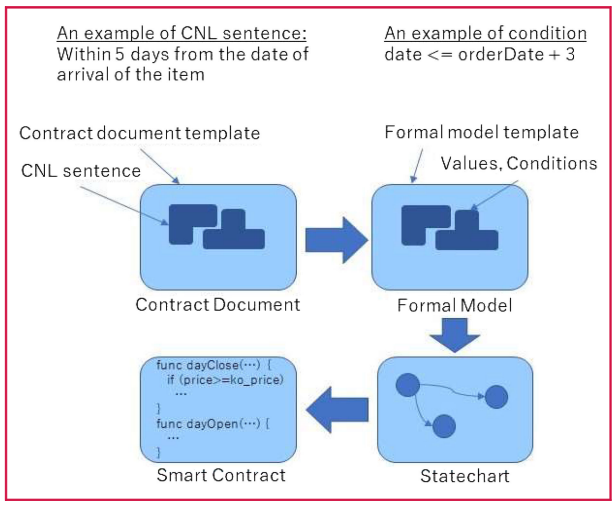


Figure 1

Template-based approach.

document is first translated into a formal model by using the formal model template that corresponds to the contract document template, as well as the rules that convert the CNL sentences into the variable part of the formal model template. The formal model is then translated into a statechart, which represents the execution model. Finally, the statechart is translated into a smart contract written in a programming language. The contract document template, the formal model template, and the conversion rule have to be defined by a human engineer in advance, but these templates and rules can be reused for a number of similar contracts. With this approach, we can reduce the development cost of creating smart contracts. In addition, the contract document is easy to understand for business people or attorneys, as it is written in a subset of natural language. In our approach, we use a state-of-the-art domain-specific language for smart contracts (DSL4SC) [3] to define the formal models of smart contracts because of its capability to define regular structural and temporal properties. In addition, we use Harel statecharts [4, 5] as the execution model of smart contracts since these statecharts are expressive enough for complex contract logics. The statecharts also help human users to review and understand the generated contract logics more easily due to the graphical representations.

In the remainder of this section, we introduce DSL4SC and statecharts with an example of a simple purchase agreement shown in **Figure 2**.

2.1 Statechart and SCXML

A statechart [4] is a diagram representing a state machine. It is often used to model the behavioral aspect of a reactive system in software development. In general, it consists of

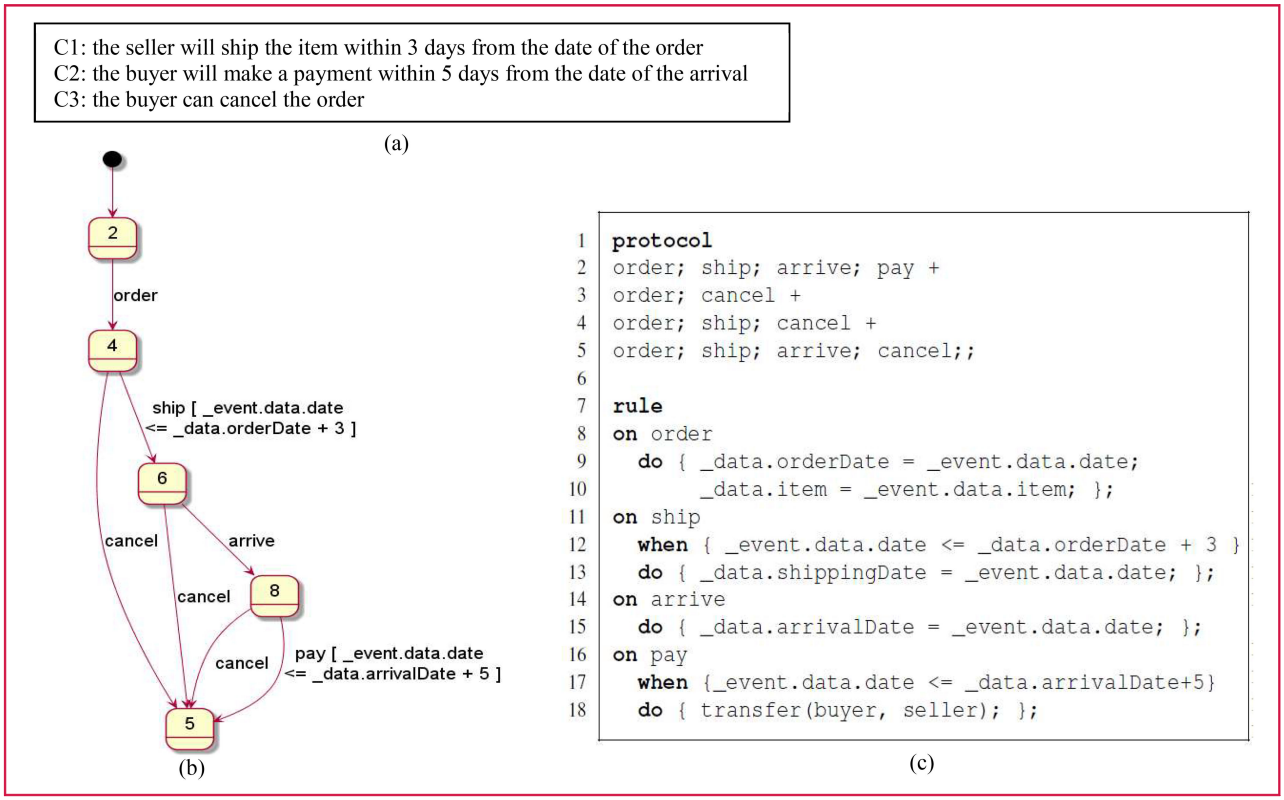


Figure 2

(a) Contract document, (b) statechart, and (c) DSL4SC model for a simple purchase agreement.

states and transitions, where each transition is defined by a rule on events, guard conditions, and actions. The states are controlled by the events. When an event is received by a system, the state of the system changes according to the current state and the definition of the transitions. In addition, the statechart can represent hierarchical states and parallel behavior. This type of state machine, which can be represented as visual diagrams, is useful for human engineers to review contract logics and communicate with business people or attorneys [6, 7].

An XML representation of a statechart is standardized by W3C, which is called State Chart XML (SCXML) [8]. SCXML provides the means of: 1) handling data in addition to states and 2) executing external scripts such as JavaScript programs to evaluate guard conditions or take actions. In this paper, we refer to an SCXML document as a statechart and use JavaScript code to handle data.

The statechart representation of a simple purchase agreement example is shown in Figure 2(b), where "`order`," "`ship`," "`arrive`," "`pay`," and "`cancel`" each refer to an event that represents a target item having been ordered, shipped, arrived, paid for, or cancelled. At the initial state denoted by the black circle, if the events "`order`," "`ship`," "`arrive`," and "`pay`" are received in this sequence, the state transitions are made in the sequence of states 2, 4, 6, 8, and then reach the final state numbered 5. In addition, at any state, the event "`cancel`" can be received and change the current state to the final state. The transitions caused by the "`ship`" and "`pay`" events have guard conditions representing "ship within 3 days" and "pay within 5 days," respectively. Here "`_event.data`" and "`_data`" respectively represent data accompanied by an event and data recorded in the statechart. The guard conditions inside the square brackets are written in JavaScript and refer to these data.

2.2 DSL4SC

DSL4SC [3] is a domain-specific language based on linear dynamic logic on finite traces ($\mathrm{LDL_f}$) [9], which can express regular structural properties and constraints on sequences of states in a state machine, while a statechart can define only procedures at each state. For instance, $\mathrm{LDL_f}$ can define a safety property, such as a proposition *always* holds, or a liveness property, such as a proposition *eventually* holds. This capability is essential for formal models of contracts because each contract defines behavioral and temporal properties such as obligations of parties.

In this section, we briefly describe the syntax and semantics of DSL4SC. A DSL4SC model is defined as a triple of a protocol, a set of properties, and a set of rules. These components are specified by the keywords "`protocol`," "`property`," and "`rule`," respectively.

"`protocol` *`pattern`*" defines a valid pattern "*`pattern`*" of event sequences to be processed in the form of a regular-expression-like notation, where sequence, choice, and iteration are represented by ";," "+," and "*," respectively.

"`property` *`LDL-formula`*" defines the properties on traces of states using an LDL formula "*`LDL-formula`*," where "`&`," "`|`," and "`!`" can be used as logical operators representing conjunction, disjunction, and negation, respectively. "`<`*`path`*`>`" and "`[`*`path`*`]`" represents modalities, where each "`path`" is a regular expression on propositions that are logical formulas representing states. Intuitively, "`<`*`path`*`>`*`p`*" represents the existence of a trace of states satisfying the regular expression "*`path`*" and its next state satisfies the proposition "*`p`*," while "`[`*`path`*`]`*`p`*" is equivalent to "`!(<`*`path`*`>!`*`p`*`)`" and states that, on any of the traces of states, if it satisfies the regular expression "`path,`" it is followed by a state satisfying "p." Therefore, the LTL formulas "`<>`p" and "`[]`p" can be seen as the LDL formulas "`<{true}`*`>`p" and "`[{true}`*`]`p" since "`{true}`" and "`{true}`*" represent "any state" and "any path," respectively.

"`rule on` *`event`* `when` *`pre-cond`* `{`*`js-cond`*`} do` *`post-cond`* `{`*`js-action`*`}`" defines an event-condition-action (ECA) rule that consists of an event, a guard condition, and an action. The guard condition is represented by an LDL formula "*`pre-cond`*" and a JavaScript program "*`js-cond`*." The action is represented by an LDL formula "*`post-cond`*" and a JavaScript program "*`js-action`*."

The DSL4SC model for the simple purchase agreement example is shown in Figure 2(c). Lines 1–5 define a protocol between a seller and a buyer. It represents that the following four event sequences are allowed: "`order;ship;arrive;pay`," "`order;cancel`," "`order;ship;cancel`," and "`order;ship;arrive;cancel`." Lines 7–17 define ECA rules. In the JavaScript programs of the ECA rules, "`_event.data`" represents data accompanied by an event, and "`_data`" represents the state machine's store. Lines 8–10 define that, when the event "`order`" is received, the JavaScript code on Lines 9 and 10 is executed and stores the order date and the item name to the state machine's store. Lines 11–13 represent that, when the "`ship`" event is received and the JavaScript condition "`_event.data.date <= orderDate+3`" holds, the JavaScript code on Line 13 is executed and records the shipping date. Lines 14 and 15 define a rule similar to Lines 8–10, which records the date of arrival. Lines 16–18 represent that the JavaScript code on Line 18 is executed when the event "`pay`" is received. The "`transfer`" function is supposed to be defined in a separate JavaScript program so that it can transfer money from the buyer to the seller where its definition is omitted in this paper.

Now, given that we add a cancellation policy C4 as shown in **Figure 3(c)**, the corresponding DSL4SC model can be defined using the propositions "`shipped`" and "`cancellable`," as shown in **Figure 3(d)**. The proposition "`shipped`" represents the states after the ordered item is shipped, while the proposition "`cancellable`" represents the states where the order can be canceled. Lines 8 and 9 represent the initial configurations of the propositions. Line 10 defines a property representing that, at any state after the item is shipped, cancel is not allowed. If we replace the property at Line 10 with "`[{true}`*`]cancellable`," it represents that cancel is allowed at any state. Lines 12–24 are the same as those of the simple purchase agreement shown in Figure 2(c) except that, on Line 18, we explicitly ensure that the next state satisfies the proposition "`shipped`." Lines 25–29 represent that, when the event "`cancel`" is received and the proposition "`cancellable`" holds, the corresponding action is executed. Lines 30–32 represent that, when the event "`cancel`" is received and the proposition "`cancellable`" does not hold, the state never changes. Line 33 represents that the values of the state variables "`shipped`" and "`cancellable`" can be changed only when the event "`ship`" is received.

3 Generation of smart contract

Our approach to generate smart contracts consists of the following three steps.

(Step 1) Translation from a contract document to a DSL4SC model.

(Step 2) Translation from a DSL4SC model to a statechart.

(Step 3) Translation from a statechart to a smart contract.

The first step requires two types of predefined templates: one for a contract document and one for a DSL4SC model. A complete contract document is created by replacing the parameters of the contract document template with actual text values written in a CNL. The text values are then converted so that the parameters of the DSL4SC model template can be replaced with the converted values. Regarding the second and the third steps, we use the techniques proposed in our earlier study [3], which describes how to generate statecharts as well as smart contracts from DSL4SC models. In the rest of this section, we focus only on the first step.

3.1 DSL4SC generation using smart contract template

A smart contract template is formalized by a triple (C, D, M), where:

T1: the seller will ship the item [SHIPPING_LEAD_TIME] from the date of the order
T2: the buyer will make a payment [PAYMENT_PERIOD]
T3: the buyer can cancel the order
T4: provided that, [LIMITATION]

(a) Contract document template

```
protocol
order; ship; arrive; pay +
order; cancel +
order; ship; cancel +
order; ship; arrive; cancel;;

property
!shipped;
cancellable;
<%- LIMITATION %>;

rule
on order do { ... };
on ship
  when { _event.data.date
       <= <%- SHIPPING_DEADLINE %> }
  do shipped { ... };
on arrive do { ... };
on pay
  when { _event.data.date
       <= <%- PAYMENT_DEADLINE %> }
  do { ... };
on cancel
  when cancellable do { ... };
on cancel
  when !cancellable do false;
except on ship
  preserve shipped, cancellable;
```

(b) DSL4SC model template

C1: the seller will ship the item within 3 days from the date of the order
C2: the buyer will make a payment within 5 days from the date of the arrival
C3: the buyer can cancel the order
C4: provided that, no cancellation is allowed after the shipment,

(c) Contract document

```
protocol
order; ship; arrive; pay +
order; cancel +
order; ship; cancel +
order; ship; arrive; cancel;;

property
!shipped;
cancellable;
[{true}*](shipped -> !cancellable);

rule
on order
  do { _data.orderDate = _event.data.date;
  _data.item = _event.data.item; };
on ship
  when { _event.data.date <= orderDate + 3 }
  do shipped
    { _data.shippingDate = _event.data.date; };
on arrive
  do { _data.arrivalDate = _event.data.date; };
on pay
  when { _event.data.date <= arrivalDate + 5 }
  do { transfer(buyer, seller); };
on cancel
  when cancellable
  do {
    _data.cancellationDate = _event.data.date;
  };
on cancel
  when !cancellable
  do false;
except on ship preserve shipped, cancellable;
```

(d) DSL4SC model

Figure 3

(a) and (c) Contract and (b) and (d) DSL4SC model for the purchase agreement with the cancellation policy.

$C(p_0 : G_0, \ldots, pn : Gn)$ is a function that represents a contract document template with parameters $p_0, \ldots, p_n$ which are to be replaced with text values complying with the corresponding CNL grammars $G_0, \ldots, Gn$;

$D(x_0, \ldots, x_m)$ is a function that represents a DSL4SC model template with parameters $x_0, \ldots, x_m$, which are different from the parameters of the contract document template; and

M is a parameter mapping that converts the $n+1$ parameter values $(t_0, \ldots, t_n)$ of the contract document template into the $m+1$ parameter values $(u_0, \ldots, u_m)$ of the DSL4SC model.

We can represent a complete contract document $C(t_0, \ldots, t_n)$ by replacing the parameters of the contract document with the CNL sentences $t_0, \ldots, t_n$. With the smart contract template (C, D, M) and the contract document $C(t_0, \ldots, t_n)$, we can compute the DSL4SC model $D(u_0, \ldots, u_m)$, where $(u_0, \ldots, u_m) = M(t_0, \ldots, t_n)$.

Examples of a contract document template and a DSL4SC model template are shown in **Figure 3(b)**, where the parameters of the contract document template are enclosed by "[" and "]" and those of the DSL4SC model template are enclosed by "<%-" and "%>." We can obtain the contract document shown in Figure 3(c) by replacing the parameters of the contract document template with the text values (e.g., "within 3 days"). Each of the text values are CNL sentences that comply with the grammar shown in **Figure 4**, which is defined using Augmented Backus–Naur Form [10]. Note that the CNL grammar for each parameter "P" (e.g., "PAYMENT_PERIOD") of the contract document template is defined as a grammar starting with a production rule named "value_P" (e.g., "value_PAYMENT_PERIOD").

```
value_SHIPPING_LEAD_TIME = period
value_PAYMENT_PERIOD     = period
value_LIMITATION         = property
period   = "within"  within_days ("day" / "days")
           [from_event_date]
within_days  = NUMBER
from_event_date = "from the date of" event
property     = "the buyer cannot cancel"
             / "the item is shipped"
             / "if" property "," property
event        = EVENT_ARRIVE / EVENT_ORDER
EVENT_ARRIVE = "arrival" / "arrival of the item"
EVENT_ORDER  = "order" / "order of the item"
NUMBER       = *("0" / ... / "9")
SKIP         = " " | "the";  skip these tokens
```

Note that the tokens of SKIP are ignored by a parser.

Figure 4

CNL syntax of the simple purchase agreement.

```
<contract>
  <placeholder name="SHIPPING_LEAD_TIME">
  within 3 days
  </placeholder>
  <placeholder name="PAYMENT_PERIOD">
  within 5 days from the date of invoice
  </placeholder>
  <placeholder name="CANCELLATION_PERIOD">
  within 7 days from the date of
  arrival of the item
  </placeholder>
  <placeholder name="CANCELLATION_POLICY">
  If the item is shipped,
  the order cannot be cancelled.
  </placeholder>
</contract>
```

```
<contract>
 <parameter name="PAYMENT_PERIOD">
  <value_PAYMENT_PERIOD
   type="Value_PAYMENT_PERIOD">
   <period type="Period">
    <token>within</token>
    <within_days type="Within_days">
      <token type="NUMBER">5</token>
    </within_days>
    <token>days</token>
    <from_event_date type="From_event_date">
     <token>from</token><token>the</token>
     <token>date</token><token>of</token>
     <event type="Event">
      <token type="EVENT_ARRIVE">
      invoice</token>
     </event>
    </from_event_date>
   </period>
  </value_PAYMENT_PERIOD>
 </parameter>
 ...
</contract>
```

Figure 5

Plain text and structured text for parameters.

The parameter mapping M is defined so that it can convert the CNL sentences into text values with which the parameters (e.g., "PAYMENT_DEADLINE") of the DSL4SC model template are replaced. Note that we can use two different sets of parameters (e.g., {"SHIPPING_LEADTIME," "PAYMENT_PERIOD," "LIMITATION"} and {"SHIPPING_DEADLINE," "PAYMENT_DEADLINE," "LIMITATION"}) for the contract document template and the DSL4SC model template. Such a mapping can be defined using a separate language such as JavaScript or XSLT.

4 Implementation

Our implementation consists of four components:

1) a CNL parser that consumes the parameter values and generates syntax trees based on the CNL grammar;
2) a smart contract template engine that generates a DSL4SC model based on a DSL4SC model template and a syntax tree;
3) a DSL4SC-to-SCXML converter that translates a DSL4SC model into an SCXML document;
4) a SCXML-to-Chaincode converter that translates an SCXML document into a chaincode, where the chaincode is an executable smart contract of Hyperledger Fabric.

4.1 CNL parser generator

The CNL parser creates a syntax tree in an XML format for each of the parameter values. It is implemented using NodeJS [11] and ANTLR4 [12]. We use ANTLR4 because it generates parsing functions, each of which represents a parsing rule defined in a grammar file. This facilitates us to choose the appropriate parsing function for each parameter. **Figure 5** shows the values of the parameters of the purchase agreement before and after parsing. Note that each parameter value is parsed on the basis of a corresponding parsing rule. For example, for the parameter "PAYMENT_PERIOD," we use the parsing rule "value_PAYMENT_PERIOD," as shown in Figure 4. The parse tree is marked up with XML tags such as "period" and "within_days," whose names are the same as the nonterminals of the grammar, so that we can easily search on the syntax tree using query languages such as XPath and XQuery.

4.2 Smart contract template engine

Our smart contract template engine (SCT) is designed to generate formal models including DSL4SC models based on formal model templates and the syntax trees of the parameter values. SCT is implemented using NodeJS and the JavaScript template library EJS [13]. Each template of the formal models is defined as an EJS template to which we introduced a special JavaScript variable "document" that refers to an XML document object model representing

```
1  <%
2  var xpath = require('xpath');
3
4  function computeDeadline(elem, defaultFrom) {
5    // construct and return expressions
6    // in the DSL4SC model
7    return expr;
8  }
9
10 var sltDeadline =
11  computeDeadline(xpath.select(
12   '//value_SHIPPING_LEAD_TIME/period',document)[0],
13   '_data.orderDate');
14 var ppDeadline  =
15  computeDeadline(xpath.select(
16   '//value_PAYMENT_PERIOD/period',document)[0]);
17 %>
18
19 protocol
20 order; ship; arrive; pay +
21 order; cancel +
22 order; ship; cancel +
23 order; ship; arrive; cancel;;
24
25 rule
26 on order
27   do { _data.orderDate = _event.data.date; };
28 on ship
29   when {_event.data.date <= <%- sltDeadline %>}
30   do { _data.shippingDate = _event.data.date; };
31 on arrive
32   do { _data.arrivalDate = _event.data.date; };
33 on pay
34   when {_event.data.date <= <%- ppDeadline %>}
35   do { ... };
```

Figure 6

EJS template for the simple purchase agreement.

the syntax trees of the parameter values. An example of an EJS template is shown in **Figure 6**. Lines 1–17 implement the parameter mapping of the purchase agreement, where XPath queries on Lines 10–16 are used to retrieve data from the XML document assigned to the variable "`document`." The text values computed by the parameter mapping are assigned to the variables "`sltDeadline`" and "`ppDeadline`," which are referred to at Lines 29 and 34, respectively.

4.3 DSL4SC to SCXML

For the translation from DSL4SC to SCXML, we use *ldltools* [3, 14]. In this translation process, a DSL4SC model excluding event names and code fragments is translated into a deterministic finite automaton (DFA) via LDL_f. The generated DFA is then translated into an SCXML document by directly mapping its states and transitions to those for the SCXML document. Event names and code fragments of the DSL4SC model are kept separately and later merged into the SCXML document.

4.4 SCXML to chaincode

The SCXML-to-chaincode converter generates a Go program that implements a chaincode interface. It consists of an SCXML document embedded in the code, an SCXML engine, and the Otto package [15], where the Otto package provides a JavaScript interpreter written in Go. With the generated chaincode, we can manage multiple instances of the contract represented by the SCXML document as if the SCXML document defines the class of the contract. Transactions to the chaincode are then mapped to events of SCXML and recorded in a ledger. JavaScript programs are then executed as actions or guard conditions by the Otto package. Since the chaincode itself cannot hold persistent data, the instances (the states and values of the data) are managed by the SCXML engine and automatically stored in the state DB, which is a key-value store (KV) that represents the current world state for the blockchain system, where the instances have unique instance keys that become the key names of the state DB. More details about the SCXML engine are described in our previous paper [3].

5 Experiments

We applied our tools to a purchase agreement and a type of derivative contract called Forward Accumulator. We first introduce the contract document templates and the DSL4SC models for these two contracts and then summarize our observations and findings.

5.1 Purchase agreement

The purchase agreement is a contract that we used as an example in the earlier sections of this paper. This agreement is to be signed by two parties: a seller and a buyer. It defines a process for purchasing items. Based on the set of parameter values shown in Figure 5 and the contract document template shown in Figure 3, the statechart shown on the left side of **Figure 7** is generated. It is then translated into a chaincode that can manage one or more instances of the statechart, as described in Section 4. For example, with the purchase agreement chaincode, we can create an instance of the statechart for each purchase order of an item to manage the lifecycle of the order. Consequently, we do not need to explicitly write JavaScript code in the DSL4SC model to manage multiple orders. Note that the transitions of the generated statechart are varied in accordance with the text value of the parameter "`CANCELLATION_POLICY`." For example, the LDL formula "`[{true}*] cancellable`" is generated from the CNL sentence "cancel is always allowed" if we use it for the parameter "`CANCELLATION_POLICY`." In this case, the statechart shown in Figure 2 is generated.

We investigated real-world purchase order examples and found that it is quite common for a single purchase order to result in multiple shipments, as the seller might ship part of the items early if the rest are not in stock and take longer to be ready. Likewise, payment is made in installments corresponding to each shipment. Considering such a realistic scenario, we should generate a statechart that can

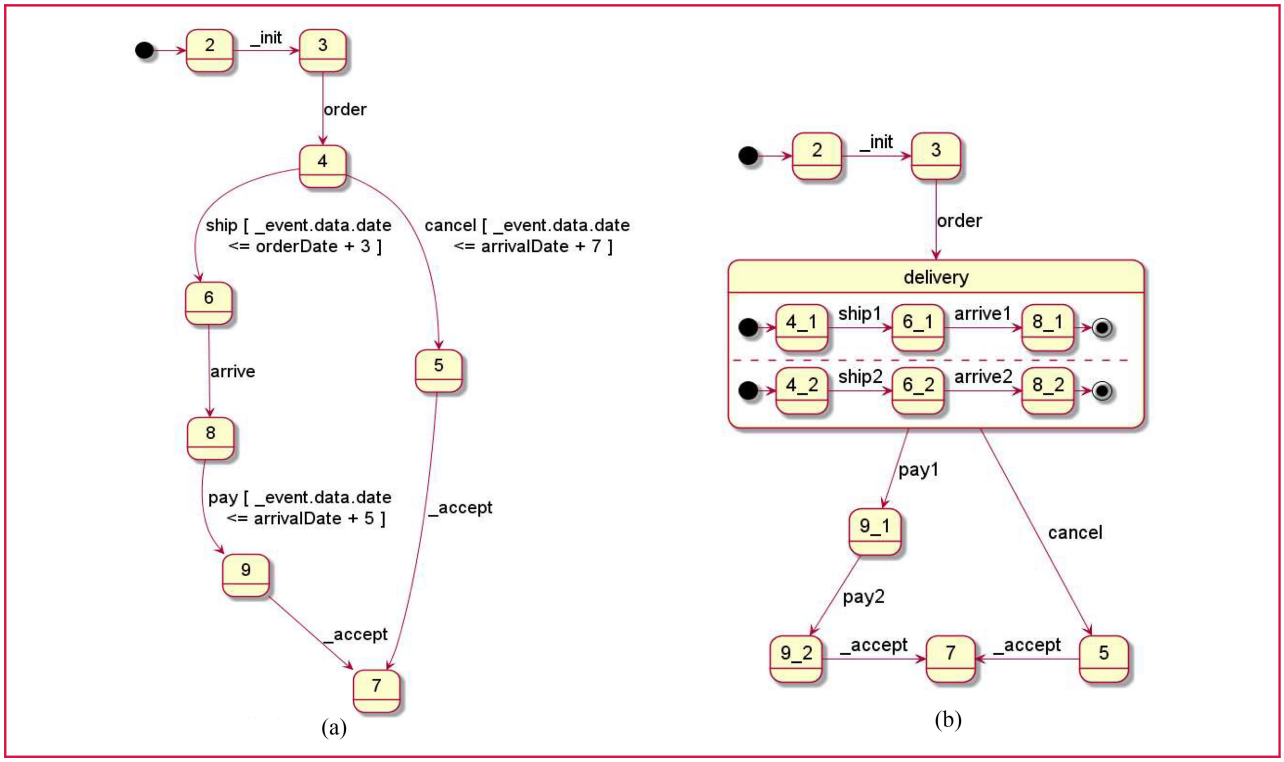


Figure 7

Statecharts of the purchase agreement. (a) No cancellation allowed after shipment. (b) Handling two items and two installments.

handle multiple shipments and installment payments. For this purpose, the statechart must individually manage the events "`ship`" and "`arrive`" for each shipped item and the number of payments. For example, the statechart shown in Figure 7(b) can handle two items and two installments. We use the parallel processes in the state "`delivery`" to represent the delivery status for each of the two items separately. We also introduce two events "`pay1`" and "`pay2`" to represents two installments. Note that the numbers of items and installments are determined when an order is placed, but neither SCXML nor DSL4SC has the capability to increase the number of states at runtime. To solve this problem, we propose: 1) using JavaScript code and variables to handle the number of payments, or 2) creating another statechart and a corresponding chaincode that represent the lifecycle of the "delivery" for each item instead of using the parallel processes. The "delivery" chaincode can communicate with the purchase agreement chaincode by using the inter-chaincode invocation mechanism of Hyperledger Fabric. Note that the performance overhead of the inter-chaincode invocation should be considered.

5.2 Forward Accumulator

Forward Accumulator [16] is a financial derivative product that obligates a buyer and a seller to exchange an underlying financial asset (e.g., security or stock) at a predefined strike price and settle it periodically within the contract period. The buyer is obligated to buy a predefined number of shares if the market price is between the strike price and the knock-out price. The contract is terminated if the market price (or the spot price) exceeds the knock-out price, while the buyer is under obligation to buy an increased number of shares than normal (i.e., multiplied by the leverage) if the market price falls below the strike price.

Figure 8 shows (a) a term sheet that specifies the conditions of a forward accumulator contract and (b) corresponding parameter-value pairs in the XML representation. Note that the knock-out condition and the strike condition are written in a controlled natural language. **Figure 9** shows (a) a DSL4SC model template that models the forward accumulator contract considering the parameters shown in Figure 8, (b) the DSL4SC model generated on the basis of the DSL4SC model template, and (c) the corresponding statechart, where the DSL4SC model shows only the ECA rules that were generated from the corresponding parameterized ECA rules. Note that the DSL4SC model and the statechart are designed to represent a contract between any two parties. In the term sheet, the buyer and the seller can be parameterized, but in the template, we do not parameterize the two. Instead, we determine those

Accumulator Forward		
Seller		Buyer
Start Date	2018-08-01 (YYYY-MM-DD)	
Termination Date	2018-12-31 (YYYY-MM-DD)	
Reference	Index	
Strike	The closing price is less than or equal to the strike price.	
Strike Price	1,300	
Knock-out	The closing price is greater than or equal to the knock-out price.	
Knock-out Price	2,000	
Shares per Day	100	
Leverage	2	

(a)

```
1  <contract>
2    <placeholder name="KNOCKOUT_CONDITION">
3    Closing Price is greater than or
4    equal to Knock-out Price.
5    </placeholder>
6    <placeholder name="STRIKE_CONDITION">
7    Closing Price is less than or
8    equal to Strike Price.
9    </placeholder>
10   <placeholder name="TERMINATION_CONDITION">
11   The contract is terminated
12   when knock-out occurs.
13   </placeholder>
14   <placeholder name="EXPIRY_DATE">
15   April 8, 2018
16   </placeholder>
17   <placeholder name="KNOCKOUT_PRICE">
18   120
19   </placeholder>
20   <placeholder name="STRIKE_PRICE">
21   100
22   </placeholder>
23   <placeholder name="LEVERAGE">
24   2
25   </placeholder>
26   <placeholder name="SHARES_PER_DAY">
27   100
28   </placeholder>
29 </contract>
```

(b)

Figure 8

(a) Term sheet and (b) parameter values for the Forward Accumulator contract.

values at runtime using the event parameters (e.g., "`_event.data.seller`") on Lines 35 and 36 of the DSL4SC model template shown in Figure 9(a). If the buyer and the seller are parameterized as template parameters, a corresponding chaincode generated from the template is effective only for the specified buyer and seller.

In the DSL4SC model template shown in Figure 9(a), the protocol of the contract is divided into two cases: 1) a normal termination case where the contract is terminated due to the expiry date, as shown in Lines 12–16, and 2) a knock-out case where the contract is terminated due to a knock-out event, as shown in Lines 18–21. These two cases are combined using the "+" ("choice") operator. The stock price is obtained from the parameter value of the event "`day_close`." The entire behavior is simply defined as "`(day_open;day_close)`*," which represents the iteration of the consecutive events "`day_open`" and "`day_close`," but we introduce the internal events whose names start with "_" (underscore) (such as "_knockout," "_expire," and "_under_strike") in order to represent the different guard conditions in the corresponding ECA rules, as shown in Lines 38–55. This is because we cannot define an ECA rule without an event, while we can define a transition without any event in an SCXML document. For example, there is a guard condition at Line 39 corresponding to the internal event "`_knockout`," which checks if the market price is greater than or equal to the knock-out price, where the value of the parameter "`koCond`" of the DSL4SC template is obtained from the value of the corresponding parameter "`KNOCKOUT_CONDITION`" shown in Figure 8. These internal events are raised in the action in Lines 60–65, which is executed when the event "`day_close`" is received. If we do not use the internal events, we must implement those logics as part of the ECA rule of the event "`day_close`" instead of raising the internal events.

5.3 Observations and findings

We now summarize our observations and findings obtained through the application to the two contracts.

5.3.1 Advantages of DSL4SC

The use of DSL4SC facilitated the implementation of parameter mappings as follows.

A property declaration can eliminate specific paths on a statechart that do not satisfy the property representing an LDL formula. In the case of the purchase agreement, we wrote the cancel policy using the property declaration to remove any paths that did not satisfy the cancel policy. If we directly generate the statechart, we must define a template of the statechart with a parameter mapping so that it can define states and transitions to satisfy the given property. This procedure is the same as what our tool performs.

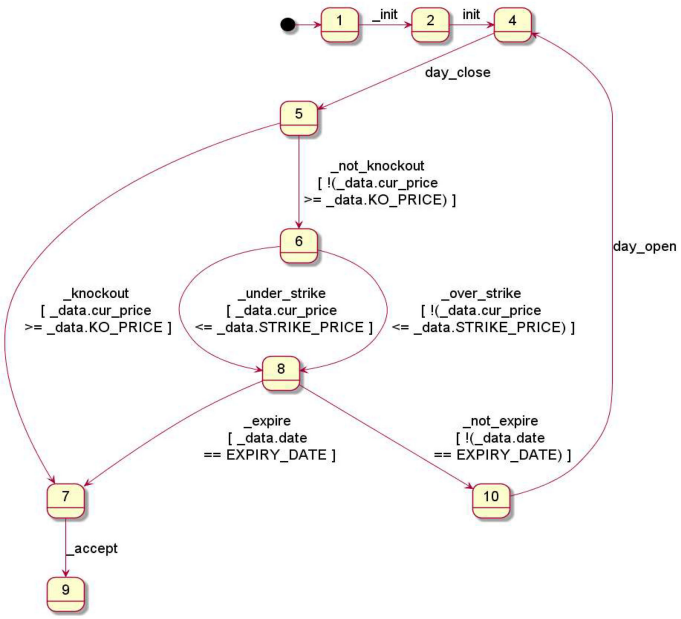
Using a protocol declaration, we can list expected scenarios in parallel and combine them using the "+" (choice) operator. The overlapping event sequences are automatically merged during the conversion from DSL4SC to SCXML. For example, in the DSL4SC model of the forward accumulator contract, we introduced two cases:

```
<%
var koPrice = ...;
var strikePrice = ...;
var expiryDate = ...;
var leverage = ...;
var sharesPerDay = ...;
var koCond = ...;
var strikeCond = ...;
%>

protocol
// normal case
init; day_close; _not_knockout;
  (_under_strike + _over_strike);
  (_not_expire; day_open; day_close; _not_knockout;
    (_under_strike + _over_strike))*; _expire
+
// knock-out case
init; day_close;
  (_not_knockout; (_under_strike + _over_strike);
   _not_expire; day_open; day_close)*; _knockout
;;

rule
on init
  do {
    _data.KO_PRICE = <%- koPrice %>;
    _data.STRIKE_PRICE = <%- strikePrice %>;
    _data.EXPIRY_DATE = <%- expiryDate %>;
    _data.SHARES_PER_DAY = <%- sharesPerDay %>;
    _data.LEVERAGE = <%- leverage %>;
    _data.cur_price = null;
    _data.date = 1;
    _data.shares = 0;
    _data.seller = _event.data.seller;
    _data.buyer  = _event.data.buyer;
  };
on _knockout
  when { <%- koCond %> }
  do { console.log("knocked_out"); };
on _not_knockout
  when { !(<%- koCond %>) };
on _under_strike
  when { <%- strikeCond %> }
  do { _data.shares =
       _data.shares + SHARES_PER_DAY*LEVERAGE; };
on _over_strike
  when { !(<%- strikeCond %>) }
  do { _data.shares =
       _data.shares + SHARES_PER_DAY; };
on _expire
  when { _data.date == EXPIRY_DATE }
  do { console.log("expired"); };
on _not_expire
  when { !(_data.date == EXPIRY_DATE) };
on day_close
  do {
    _data.cur_price = _event.data.price;
    // consecutive internal events
    __raiseEvent("_knockout");
    __raiseEvent("_not_knockout");
    __raiseEvent("_under_strike");
    __raiseEvent("_over_strike");
    __raiseEvent("_expire");
    __raiseEvent("_not_expire");
  };
on day_open
  do { _data.date = _data.date + 1; };
```

(a)

```
rule
on init
  do {
    _data.KO_PRICE = 120;
    _data.STRIKE_PRICE = 100;
    _data.EXPIRY_DATE = 8;
    _data.SHARES_PER_DAY = 100;
    _data.LEVERAGE = 2;
    _data.cur_price = null;
    _data.date = 1;
    _data.shares = 0;
    _data.seller = _event.data.seller;
    _data.buyer  = _event.data.buyer;
  };
on _knockout
  when { _data.cur_price >= _data.KO_PRICE }
  do { console.log("knocked_out"); };
on _not_knockout
  when { !(_data.cur_price >= _data.KO_PRICE) };
on _under_strike
  when { _data.cur_price <= _data.STRIKE_PRICE }
  do { _data.shares =
       _data.shares + SHARES_PER_DAY*LEVERAGE; };
on _over_strike
  when { !(_data.cur_price <= _data.STRIKE_PRICE)}
  do { _data.shares =
       _data.shares + SHARES_PER_DAY; };
```

(b)



(c)

Figure 9

Templates and models for forward accumulator. (a) DSL4SC model template. (b) DSL4SC model. (c) Statechart.

termination by expiry date and termination by knock-out event. We then combined them using the "+" operator. The resulting statechart [see Figure 9(c)] contains states 4, 5, 6, 8, and 10, which are shared by the two termination cases represented by the transition from 5 to 7 and the transition from 8 to 7. This capability is useful when we parameterize a part of the regular expression pattern of events.

5.3.2 Design choice of smart contract template

We do not suggest replacing all variable portions of a contract document with template parameters. Rather, we must carefully define the template parameters by considering when parameter values should be determined, from the viewpoint of reusability of a generated smart contract and efficiency of its execution. For example, in the

case of the forward accumulator contract, the seller and the buyer are parameterized as the JavaScript variables in the DSL4SC model instead of template parameters, where the values of the JavaScript variables are given by the event. On the other hand, if we use template parameters representing the seller and the buyer, those values are hard-coded in a generated smart contract, as the template parameters are instantiated when the smart contract is generated. In addition, we cannot create a new state of a statechart at runtime, as described in Section 5. In order to handle such dynamically created states, we can use a JavaScript variable. However, it is difficult to visualize such dynamically created states using a diagram such as the UML state diagram, and the visualization is required for engineers to communicate with business persons and attorneys. If there is a requirement to dynamically create concurrent processes, we suggest using a mechanism of a blockchain platform to invoke another smart contract.

5.3.3 Expressiveness of controlled natural language

ANTLR4 covers only the subset of context-free grammar. It cannot handle the context of CNL sentences. Therefore, if we need to handle pronouns such as "it," we should define a parameter mapping so as to determine those meanings for each parameter. Another solution is to use natural language processing (NLP) technologies to determine the meanings of the pronouns. Our smart contract template framework is flexible enough to use NLP technologies as part of the parameter mapping. Note that we must take care regarding its ambiguity, which should be avoided from the perspective of generating executable smart contracts.

In addition, terms themselves (e.g., "knock-out") are often defined and referred to in the contract. If we parameterize such terms, we need to handle them as if they are declarations of variables, as in the case of programming languages.

6 Related work

6.1 Smart contract template

The Ricardian contract [17] is a concept of digitizing legal contracts. It offers a system for recording digitally signed legal contract documents in a human-readable and machine-readable format. Clack et al. [18] presented an implementation design based on the Ricardian contract, where the parameters of templates have the role of connecting legal proses with executable code. They also proposed having each of the parameters consist of ID, type, and value. In contrast, our approach utilizes the notions of "grammar" and "parameter mapping" rather than "type."

R3 Corda [19] is a blockchain implementation that realizes the concept of the Ricardian contract. It has a function to record human-readable legal prose documents linked to executable smart contracts. The Cicero project [20] aims to establish standards for smart contract templates and provide reusable domain-specific contract templates.

6.2 Models and languages for contracts

Flood et al. [6] proposed finite state automata to represent financial contracts and discussed the advantages of using the finite state automata. Azzopardi et al. [7] proposed a secure smart contract language based on the finite state machine and developed a graphical interface for their language.

Hvitved [1] proposed a DSL based on a trace-based contract model to handle various aspects of contracts including obligations, permissions, and reparation. Ergo [21] is another domain-specific language that captures the execution logic of legal contracts. Its syntax is designed to be more accessible to lawyers.

7 Conclusion

We have presented a technique to generate an executable smart contract from a human-understandable contract document. The automation is enabled by a smart contract template consisting of a document template, a DSL4SC template, and a parameter mapping between them. We developed a set of tools, applied them to two case studies, and summarized our observations including the advantages of the use of DSL4SC.

As the use of smart contract is becoming increasingly prevalent, the need for easier and faster development of accurate and safe smart contract increases. We believe that the automated smart contract generation will be one of the key technologies in the future of blockchain.

References

1. T. Hvitved, "Contract formalisation and modular implementation of domain-specific languages," Ph.D. thesis, Univ. Copenhagen, Copenhagen, Denmark, 2012.
2. Understanding the DAO attack. 2016. [Online]. Available: http://www.coindesk.com/understanding-dao-hack-journalists/
3. N. Sato, T. Tateishi, and S. Amano, "Formal requirement enforcement on smart contracts based on linear dynamic logic," in *Proc. IEEE Conf. Internet Things, Green Comput. Commun. Cyber Physical Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. Congr. Cybern.*, pp. 945–954, 2018.
4. J. Rumbaugh, I. Jacobson, and G Booch, *Unified Modeling Language Reference Manual*. London, U.K.: Pearson Higher Educ., 2004.
5. D. Harel, "Statecharts: A visual formalism for complex systems," *Sci. Comput. Program.*, vol. 8, pp. 231–274, 1987.
6. M. D. Flood and O. R. Goodenough, "Contract as automaton: The computational representation of financial agreements," Office of Financial Research Working Paper No. 15-04, 2015.
7. A. Mavridou and A. Laszka, "Designing secure ethereum smart contracts: A finite state machine based approach," in *Proc. 22nd Int. Conf. Financial Crytography Data Secur.*, 2018.
8. J. Barnett, R. Akolkar, R. J. Auburn, et al., "State Chart XML (SCXML): State machine notation for control abstraction," W3C, Cambridge, MA, USA, 2015.
9. G. D. Giacomo and M. Y. Vardi, "Linear temporal logic and linear dynamic logic on finite traces," in *Proc. 23rd Int. Joint Conf. Artif. Intell.*, 2013, pp. 854–860.
10. Augmented BNF for Syntax Specifications: ABNF, IETF RFC 5234, 2008. [Online]. Available: https://tools.ietf.org/rfc/rfc5234.txt
11. NodeJS. 2018. [Online]. Available: https://nodejs.org/
12. NTLR. 2018. [Online]. Available: http://www.antlr.org

13. Embedded JavaScript templates (EJS). 2018. [Online]. Available: https://github.com/mde/ejs
14. ldltools. 2018. [Online]. Available: https://github.com/ldltools
15. Otto. 2018. [Online]. Available: https://github.com/robertkrimen/otto
16. K. Lam, P. L. H. Yu, and L. Xin, "Accumulator pricing," in *Proc. IEEE Symp. Comput. Intell. Financial Eng.*, 2009, pp. 72–79.
17. I. Grigg, "The Ricardian contract," in *Proc. Workshop Electron. Contracting*, 2004, https://ieeexplore.ieee.org/document/1319505?arnumber=1319505
18. C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: Foundations, design landscape and research directions," arXiv: 1608.00771, 2016.
19. R. G. Brown, J. Carlyle, I. Grigg, et al., "Corda: An introduction." 2019. [Online]. Available: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf
20. The Cicero project, 2018. [Online]. Available: https://docs.accordproject.org/docs/cicero.html
21. The Ergo project, 2018. [Online]. Available: https://docs.accordproject.org/docs/ergo.html

Received May 31, 2018; accepted for publication February 1, 2019

Takaaki Tateishi *IBM Research – Tokyo, Tokyo 103-8510, Japan* (*tate@jp.ibm.com*). Dr. Tateishi received a Ph.D. degree in information science from Japan Advanced Institute of Science and Technology, Nomi, Japan, in 2003. He is a Research Staff Member with the FSS and Blockchain Solutions group, IBM Research – Tokyo, Tokyo, Japan. He joined IBM Research – Tokyo in 2003, where he worked on program analysis, legacy transformation, and Web application security.

Sachiko Yoshihama *IBM Research – Tokyo, Tokyo 103-8510, Japan (sachikoy@jp.ibm.com).* Dr. Yoshihama received an M.S. degree in information security from the Institute of Information Security, Yokohama, Japan, in 2007, and a Ph.D. degree from Yokohama National University, Yokohama, in 2010. She is a Senior Technical Staff Member and Senior Manager with the FSS and Blockchain Solutions group, IBM Research – Tokyo, Tokyo, Japan. She joined IBM Research – Tokyo in 2003 as a Research Staff Member, where she worked on security technologies such as trusted computing, information flow control, Web application security, and data leakage prevention. She is a member of the ACM and the IBM Academy of Technology.

Naoto Sato *IBM Research – Tokyo*, *Tokyo 103-8510, Japan (hito@jp.ibm.com)*. Dr. Sato received a Ph.D. degree in computer science from the University of Tokyo, Tokyo, Japan, in 1997. He is a Research Staff Member with the FSS and Blockchain Solutions group, IBM Research – Tokyo, Tokyo. Since he joined IBM Research in 2001, he has been working on several research and development projects including a XQuery JIT compiler development project.

Shin Saito *IBM Research – Tokyo, Tokyo 103-8510, Japan* (*shinsa@jp.ibm.com*). Mr. Saito received an M.S. degree in computer science from the University of Tokyo, Tokyo, Japan, in 2001. He is a Research Staff Member with the FSS and Blockchain Solutions group, IBM Research – Tokyo, Tokyo. He joined IBM in 2001. He technically led a number of Blockchain projects and is working on verification of Blockchain consensus protocols.