

A TOKEN BASED TRANSLATOR TO CONVERT BPMN TO SOLIDITY SMART CONTRACTS

Govinnage Rasika Perera

(168250J)

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

April 2020

A TOKEN BASED TRANSLATOR TO CONVERT BPMN TO SOLIDITY SMART CONTRACTS

Govinnage Rasika Perera

(168250J)

Thesis submitted in partial fulfillment of the requirements for the degree
Master of Science in Computer Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

April 2020

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature:

Date:

Name: G R Perera

The supervisor/s should certify the thesis/dissertation with the following declaration.

I certify that the declaration above by the candidate is true to the best of my knowledge and that this report is acceptable for evaluation for the MSc Research Thesis.

Signature of the supervisor:

Date:

Name: Dr. Indika Perera

Acknowledgement

I would like to place record my deepest gratitude to Dr. Indika Perera in Department of Computer Science and Engineering, University of Moratuwa for the generous and invaluable guidance, suggestions and help provided to fulfil this research. Allowing me to experiment and explore my own and steps are altered whenever needed is a great fortunate I received. Thus, I would like to appreciate the guidance and allocating his precious time for my research throughout the whole time.

Also, I would like to thank Dr. Charith Chitraranjan, Department of Computer Science and Engineering, University of Moratuwa for co-ordinating the research and allocating his time for these works.

Last, but definitely not the least I wish to extend my sincere appreciation to Mrs. D. N. Perera (My Wife) for her inspiration and inputs for this research and all the hardships she went through to make this research a success. I have no valuable words to express my thanks for the all those people who helped me in this research in various aspects to make this dissertation possible.

Table of Contents

Declaration	3
Abstract	4
Acknowledgement	6
Table of Contents	7
List of Figures	9
List of Tables	11
List of Abbreviations	12
List of Appendices	12
1. INTRODUCTION.....	13
1.1. Problem Statement.....	15
1.2. Goals and Objectives.....	16
1.3. Scope and Limitations	16
1.4. Research Contributions.....	17
2. LITERATURE REVIEW.....	18
2.1. A brief introduction to the Smart Contracts.....	18
2.2. Analysis of Business Process Modelling (BPM) Techniques	19
2.3. Analysis of Modeling Tools & Plugins for BPMN	24
2.4. Analysis of BPMN 2.0 Specification and Solidity Language.....	25
2.5. Existing Systems	26
2.6.1. Caterpillar	26
2.6.2. Unibright	26
2.6.3. Petri-Nets Translation and Reduction Approach.....	27
2.6.4. Choreography Diagrams Approach.....	28
2.6.5. Extended Choreography Diagrams Approach	29
3. RESEARCH METHODOLOGY	30
3.1. High Level Steps of the Research Methodology.....	30
3.2. Data Collection.....	31
3.3. Implementation of the Translator.....	32
3.3.1. BPMN Modeler Integration.....	33
3.3.2. BPMN to Solidity Translation.....	33
3.4. BPMN-to-Solidity Abstract Syntax Tree (AST) Transformation	38
3.4.1. BPMN Sub-Models to Solidity Mapping.....	41
3.4.2. BPMN Elements to Solidity Mapping	43
3.4.3. BPMN Representation of Solidity Top Level Constructs.....	56
4. EVALUATION AND RESULTS	60

4.1.	Translator Evaluation	60
4.1.1.	Abstract Features Matching in BPMN and Solidity	60
4.1.2.	Conducting a Survey for a Selected User Group.....	62
4.2.	Re-generated Solidity Smart Contract Code Evaluation	68
4.3.	Comparative Analysis with the Existing Systems	72
4.3.1.	Caterpillar	72
4.3.2.	Unibright	73
4.3.3.	Petri-Nets Translation and Reduction Approach.....	75
4.3.4.	Choreography Diagrams Approach.....	76
4.3.5.	Extended Choreography Diagrams Approach	77
4.3.6.	Comparative Analysis of the Diagrams	80
4.3.7.	Comparative Analysis of the Generated Solidity Codes.....	86
4.4.	Input BPMN Diagrams and Re-generated Solidity Codes	92
4.4.1.	Rental Agreement.....	92
4.4.2.	Marriage: Wedding Gift.....	95
4.4.3.	Sellable.....	95
4.4.4.	Lottery.....	97
4.4.5.	Basic Token	99
4.4.6.	Crowd Sale	100
4.5.	Gap Analysis of the Supported BPMN 2.0 Constructs	103
4.6.	Gap Analysis of the Supported Solidity Constructs.....	104
4.6.	BPMN 2.0 Modelling Recommendations.....	106
4.7.	Chapter Conclusion.....	107
5.	Conclusion and Future Work.....	108
5.1.	Conclusion.....	108
5.2.	Limitation and Future Work.....	110
	References.....	112
6.	Appendices	115
A1.	Unibright Workflow Designer generated Solidity Code for the Demo Workflow Example	115
B1.	Process Model XML Source for the Loan Assessment Example Using Caterpillar v3.0	121
B2.	Process Model XML Source for the Loan Assessment Example Using Proposed Approach.....	128
C1.	Generated Smart Contract for Loan Assessment Example Using Caterpillar.....	137
C2.	Generated Smart Contract for Loan Assessment Example Using Proposed Approach.....	148
D1:	Truffle Test Written for Invoice Handling Smart Contract.....	150
D2:	Truffle Test Written for Lottery Smart Contract.....	151

List of Figures

Figure 2.1: Structure of the literature review.....	18
Figure 2.2: A Process Model Example in Caterpillar [13].....	26
Figure 2.3: Multiparty Approval Example using Unibright.....	27
Figure 2.4: An example of PetriNets Translation and Reduction Approach [16]	28
Figure 2.5: A Supply Chain Example using Choreography Based Approach [17].....	28
Figure 2.6: A Rental Agreement Example [7] using Extended Choreography Diagrams	29
Figure 3.1: High level view of the Research Methodology	30
Figure 3.2: Crowdsale Solidity Smart Contract	31
Figure 3.3: Sequence Diagram Representation of Crowd Sale Example..	32
Figure 3.4: Top Level View of BPMN to Solidity Translator.....	34
Figure 3.5: ANLRv4 Parser Generation for BPMN XML.....	35
Figure 3.6: BPMN ANTLR g4 Grammar	35
Figure 3.7: BPMN ANTLR g4 Lexer	36
Figure 3.8: Hello-World Example	38
Figure 3.9: BPMN Process Model for the Hello-World Example.....	39
Figure 3.10: Configure A Return Text for the Hello-World Task	39
Figure 3.11: An Excerpt of Hello-World Example's BPMN XML.....	40
Figure 3.12: HelloWorld example's BPMN AST.....	41
Figure 3.13: HelloWorld example's Solidity AST	41
Figure 3.14: BPMN private process example	42
Figure 3.15: BPMN public process example	42
Figure 3.16: An Example for Start Events and End Events.....	43
Figure 3.17: Solidity Code for Start Event and End Event Example	44
Figure 3.18: Configuring Conditional Start Event	44
Figure 3.19: An Example for the Conditional Start Events	45
Figure 3.20: Solidity Code for the Conditional Start Event Example	45
Figure 3.21: Configuring Message for Escalation Event.....	46
Figure 3.22: Throw Event with Escalation Event Definition Example ...	46
Figure 3.23: Soldity Code for the Throw Event with Escalation Event Definition	48
Figure 3.24: Generic Tasks Example.....	48
Figure 3.25: Configuring Documentation for BPMN Elements.....	49
Figure 3.26: Solidity Code for Tasks Example.....	49
Figure 3.27: Example for Script Task.....	50
Figure 3.28: Configuring Script Value of the Script Task.....	50
Figure 3.29: Solidity Code for Script Task.....	52
Figure 3.30: Example for Send Task.....	52
Figure 3.31: Configuring Input Data Mapping for Send Task.....	53

Figure 3.32: Solidity Code for Send Task Example	53
Figure 3.33: Configuring Incoming Message for Receive Task	54
Figure 3.34: Example for Receive Task	54
Figure 3.35: Solidity Code for the Receive Task	55
Figure 3.36: Data Objects and Data Store References Example	56
Figure 3.37: Solidity Code for Data Objects and Data Store References Example	56
Figure 3.38: Solidity Top-Level Constructs Example.....	57
Figure 3.39: Solidity Code for the Top-Level Constructs Example	57
Figure 4.1: BPMN to Solidity Translator Evaluation Using Abstract Features	60
Figure 4.2: Summary of the BPMN Knowledge Ratings.....	63
Figure 4.3: Summary of the Programming Skills Ratings.....	63
Figure 4.4: Summary of the Solidity Language Ratings	64
Figure 4.5: Summary of the Readability of the Input Diagram.....	64
Figure 4.6: Summary of the Correctness of the Business Logic	65
Figure 4.7: Summary of the Correctness of the State Transitions.....	66
Figure 4.8: Summary of the Correctness of the Entry Points	67
Figure 4.9: Truffle Test Written for the Basic Token Smart Contract.....	70
Figure 4.10: Test Execution Output of the Tests Written in Truffle.....	71
Figure 4.11: Annotating Solidity Variables in BPMN Diagram in Caterpillar	73
Figure 4.12: Unibright excerpt code for the multi-party approval template example (complete code is available in Appendix A, page 115)	75
Figure 4.13: An Excerpt of the Generated Solidity Code in [16]	76
Figure 4.14: Process Instance Contract Implementation Templating Algorithm [18]	76
Figure 4.15: Code of the Generated Common Interface (excerpt)	77
Figure 4.16: BPMN Diagram of the Loan Assessment Process Model using Caterpillar [13].....	81
Figure 4.17: Solidity Annotations Required for the Global Process Level in Caterpillar	81
Figure 4.18: Solidity Annotations Required for the ‘Enter Loan Application’ Task in Caterpillar.....	82
Figure 4.19: Solidity Annotation Syntax for the Tasks in Caterpillar [13]	82
Figure 4.20: BPMN Diagram of the Loan Assessment Process using the Proposed Approach.....	82
Figure 4.21: Summary of Metrics Results of the Total Solidity Contract Complexity	90
Figure 4.22: Summary of the Average Metrics Results of Solidity Contract Complexity	90
Figure 4.23: Truffle Framework Output of the Deployment of Contracts	91

Figure 4.24: BPMN Diagram for the Rental Agreement Business Contract	93
Figure 4.25: Re-generated Solidity Code for the Rental Agreement Business Contract.....	94
Figure 4.26: BPMN Diagram for the Marriage_Wedding Gift Business Contract	95
Figure 4.27: Re-generated Solidity Code for the Marriage_Wedding Gift Business Contract.....	95
Figure 4.28: BPMN Diagram for the Sellable Business Contract	96
Figure 4.29: Re-generated Solidity Code for the Sellable Business Contract	97
Figure 4.30: BPMN Diagram for the Lottery Business Contract	98
Figure 4.31: Re-generated Solidity Code for the Lottery Business Contract	99
Figure 4.32: BPMN Diagram for the Basic Token Business Contract	100
Figure 4.33: Re-generated Solidity Code for the Basic Token Business Contract	100
Figure 4.34: BPMN Diagram for the Crowd Sale Business Contract	101
Figure 4.35: Re-generated Solidity Code for the Crowd Sale Business Contract	103
Figure 4.36: Abstract BPMN Diagram for the Crowd Sale.....	106

List of Tables

Table 2.1: Criterion for the Business Process Modelling Techniques Comparison [10]	19
Table 2.2: Business Modeling Techniques (BPM) Comparison [10]	21
Table 2.3: BPMN Modelling Tools & Plugins Comparison [11]	24
Table 4.1: A List of Abstract Features in BPMN and Solidity.....	61
Table 4.2: Summary of Abstract Feature Matching in BPMN XML and Solidity	61
Table 4.3: Details of the Participant	62
Table 4.4: Example Input and Output of the Translator	62
Table 4.5: Sample Contracts against Covered BMPN Elements.....	72
Table 4.6: Summary of the Similar Translators.....	78
Table 4.7: Loan Assessment Steps Comparison	83
Table 4.8: Solidity Source Code Metrics for Smart Contracts [21].....	86
Table 4.9: Cyclomatic Complexity Recommendations [22]	88
Table 4.10: Generated Solidity Code Complexity Analysis Metrics Results	89
Table 4.11: Deployment Gas consumption Identification	92
Table 4.12: Gap Analysis of the Supported BPMN 2.0 Constructs	103
Table 4.13: Gap Analysis of the Solidity Language Constructs Supported	104
Table 6.1: Detailed Responses for the Survey Study.....	152

List of Abbreviations

BPM	:	Business Process Model
BPMN	:	Business Process Modelling Notation
XML	:	Extensible Markup Language
XSD	:	XML Schema Definition
AST	:	Abstract Syntax Tree
PoC	:	Proof Of Concept
SLOC	:	Source Lines of Code
LLOC	:	Logic Lines of Code

List of Appendices

Appendix A: Unibright Workflow Designer Generated Solidity Code....	115
Appendix B: Diagram Source for the Loan Assessment Example using Caterpillar and Proposed Approach.....	121
Appendix C: Generated Solidity Code for the Loan Assessment Example using Caterpillar and Proposed Approach.....	137
Appendix D: Truffle Test Cases for the Generated Code.....	150
Appendix E: Detailed Responses of the Survey.....	152