Towards Modeling Privity and Enforceability Requirements for BPM based Smart Contracts

Julius Köpke[1]

Abstract: Blockchains are a good foundation for the realization of inter-organizational business processes and smart contracts. Existing approaches for BPM on blockchains focus on supporting observability and enforceability. However, they fall short in providing privity. Since there are tradeoffs between privity, enforceability and costs, we propose to explicitly model privity and enforceability requirements for BPM based blockchain approaches. Such extended models are the foundation for detecting conflicts, to balance conflicting requirements, and to derive compliant implementations.

Keywords: Blockchain; Distributed ledger; Privity; Privacy; Enforceability; Conceptual Modeling; Business Process Modeling

1 Introduction

Blockchain technology has gained attention in the Business Process Management community in the recent years [Di19, Me18]. On the one hand, blockchains are seen as a good basis for inter-organizational business processes. On the other hand methods from the business process management community are considered as a good foundation for the model-driven development of smart contracts on blockchains [LW19, Hu16].

Smart contracts, originally introduced in [Sz97] have the objectives observability, privity and enforceability. Blockchains naturally provide a good basis for addressing observability and enforceability requirements. This is also witnessed by numerous approaches for executing business process models on blockchains (see [Di19, Hä18b, St19] for some examples) focusing on these aspects.

Privity describes the property that knowledge about the contract should only be spread to the participants with a contractual need to know. However, this property is not addressed by existing approaches or rather simple assumptions like encrypting all data or using off-chain data are proposed.

In our earlier work [KFE19] we defined privity spheres of data items in order to express privity requirements of business processes. Such spheres limit the read-access of data-values to certain sets of participants. In particular, the most general public sphere allows the entire

[1] Department of Informatics Systems, Alpen-Adria-Universität Klagenfurt, Austria, Julius.Koepke@aau.at

blockchain network to read the data. The most restricted sphere only allows participants to read some data value if they will certainly need the data for some future step.

However, following the existing approaches for BPM on blockchain, limiting access to data items has negative impacts on enforceability. I.e. when data referenced by some decision node is encrypted or stored off-chain, the blockchain network fails short in validating the correctness of the decision [Ha18a]. This problem can be tackled in a reactive manner as proposed in [Ha19], where encrypted data is only revealed in case of a dispute. For supporting proactive enforcement, we have proposed solutions based on voting schemes in [KFE19]. Following these solutions, the larger the set of participants with data access for some decision, the larger the potential set of voters. This requires to balance the requirements on enforceability and privity.

2 Implementing Privity and Enforceability Requirements

In the talk, we will report on our current work on annotating process models with privity- and enforceability requirements. Having such extended models allows to derive optimized implementations using encryption and voting schemes on public blockchains as sketched in [KFE19]. However, alternative implementations using private/permissioned chains or Zero Knowledge Proofs such as [Gr16, Be19] are also viable options. In the talk, we will comment on these alternatives and discuss their strength and weaknesses. I.e. implementing the most restrictive privity sphere efficiently on a permissioned blockchain with channels can be challenging as the channel to write the data to may depend on runtime decisions that are taken after the data should be written. The applicability of Zero Knowledge Proofs has recently made significant advances [ET18]. However, these methods still come with substantial amounts of costs in terms of CPU time, RAM, storage space and gas costs. Consequently, there is no simple one-size fits all solution and implementation decisions should be grounded on requirements for privity and on enforceability.

We currently aim in restricting read access to data elements. Potential future work is to additionally encrypt or obfuscate the control-flow in the spirit of [MGC19, HGF12].

References

[Be19] Ben-Sasson, Eli; Bentov, Iddo; Horesh, Yinon; Riabzev, Michael: Scalable Zero Knowledge with No Trusted Setup. In (Boldyreva, Alexandra; Micciancio, Daniele, eds): Advances in Cryptology – CRYPTO 2019. Springer, pp. 701–732, 2019.

[Di19] Di Ciccio, Claudio; Cecconi, Alessio; Dumas, Marlon; García-Bañuelos, Luciano; Pintado, Orlenys; Lu, Qinghua; Mendling, Jan; Ponomarev, Alexander; Tran, An Binh; Weber, Ingo: Blockchain Support for Collaborative Business Processes. Informatik Spektrum, 05 2019.

[ET18] Eberhardt, J.; Tai, S.: ZoKrates - Scalable Privacy-Preserving Off-Chain Computations. In: 2018 IEEE International Conference on Internet of Things (iThings) and GreenCom and CPSCom and SmartData. pp. 1084–1091, July 2018.

[Gr16] Groth, Jens: On the Size of Pairing-Based Non-interactive Arguments. In (Fischlin, Marc; Coron, Jean-Sébastien, eds): Advances in Cryptology – EUROCRYPT 2016. Springer, pp. 305–326, 2016.

[Ha18a] Haarmann, Stephan; Batoulis, Kimon; Nikaj, Adriatik; Weske, Mathias: DMN Decision Execution on the Ethereum Blockchain. In: CAiSE'18. pp. 327–341, 2018.

[Hä18b] Härer, Felix: Decentralized business process modeling and instance tracking secured by a Blockchain. In: ECIS2018. 2018.

[Ha19] Haarmann, Stephan; Batoulis, Kimon; Nikaj, Adriatik; Weske, Mathias: Executing Collaborative Decisions Confidentially on Blockchains. In: Business Process Management: Blockchain and Central and Eastern Europe Forum. Springer, 2019.

[HGF12] Hans-Georg; Fill, Hans-Georg: Using Obfuscating Transformations for Supporting the Sharing and Analysis of Conceptual Models. Multikonferenz Wirtschaftsinformatik 2012 - Tagungsband der MKWI 2012, 01 2012.

[Hu16] Hull, Richard; Batra, Vishal S.; Chen, Yi-Min; Deutsch, Alin; III, Fenno F. Terry Heath; Vianu, Victor: Towards a Shared Ledger Business Collaboration Language Based on Data-Aware Processes. In: ICSOC 2016. pp. 18–36, 2016.

[KFE19] Köpke, Julius; Franceschetti, Marco; Eder, Johann: Balancing Privity and Enforceability of BPM-Based Smart Contracts on Blockchains. In: Business Process Management: Blockchain and Central and Eastern Europe Forum. Springer, 2019.

[LW19] Ladleif, Jan; Weske, Mathias: A Unifying Model of Legal Smart Contracts. In: Conceptual Modeling - 38th International Conference, ER 2019, Salvador, Brazil, November 4-7, 2019, Proceedings. pp. 323–337, 2019.

[Me18] Mendling, Jan; Weber, Ingo; van der Aalst, Wil M. P.; et al.: Blockchains for Business Process Management - Challenges and Opportunities. ACM Trans. Management Inf. Syst., 9(1):4:1–4:16, 2018.

[MGC19] Martínez, Salvador; Gerard, Sebastien; Cabot, Jordi: On the Need for Intellectual Property Protection in Model-Driven Co-Engineering Processes. In: Enterprise, Business-Process and Information Systems Modeling. Springer International Publishing, Cham, pp. 169–177, 2019.

[St19] Sturm, Christian; Scalanczi, Jonas; Schönig, Stefan; Jablonski, Stefan: A Blockchain-based and resource-aware process execution engine. Future Generation Computer Systems, 100:19 – 34, 2019.

[Sz97] Szabo, Nick: Formalizing and Securing Relationships on Public Networks. First Monday, 9(2), 1997.