Modelling principles for blockchain-based implementation of business or scientific processes

Mantas Jurgelaitis
Information Systems Department
Kaunas University of Technology,
Informatics Faculty
Kaunas, Lithuania
mantas.jurgelaitis@ktu.lt

Vaidotas Drungilas
Information Systems Department
Kaunas University of Technology,
Informatics Faculty
Kaunas, Lithuania
vaidotas.drungilas@ktu.lt

Lina Čeponienė
Information Systems Department
Kaunas University of Technology,
Informatics Faculty
Kaunas, Lithuania
lina.ceponiene@ktu.lt

Rita Butkienė
Information Systems Department
Kaunas University of Technology,
Informatics Faculty
Kaunas, Lithuania
rita.butkiene@ktu.lt

Evaldas Vaičiukynas
Information Systems Department
Kaunas University of Technology,
Informatics Faculty
Kaunas, Lithuania
evaldas.vaiciukynas@ktu.lt

***Abstract*—Blockchain technology and smart contract development currently lacks clarity in its implementation. The complicated architecture of blockchain is an obstacle that developers face during design and implementation of blockchain-based systems. In this paper we propose a method based on Model Driven Architecture, which could be used for defining and specifying blockchain structure and behavior. Such approach could be used as one of the ways for describing blockchain-based systems in a more general language in order to facilitate blockchain development process.**

***Keywords*—blockchain, smart contract, MDA, UML**

I. Introduction

Blockchain is a decentralized, distributed database that is shared and replicated across all the parties participating in the network. It takes a form of a public ledger for the transactions contained in the chain [1]. The blockchain is made up of blocks, where each block contains a hash of the previous block, thus linking to it [2]. The main advantages provided by the blockchain are a peer-to-peer exchange (i.e. decentralization) and robust public record keeping with the possibility to eliminate the intermediary between parties [3].

Blockchain enables development of distributed software architecture where networks of untrusted participants can establish agreements on shared states for decentralized and transactional data in a secure way. Blockchain ensures trust among parties in decentralized systems without the need of centralized supervisor in charge of verifying the correctness of the records in the ledger [4]. Since blockchain digital currencies combine features of money with those of a payment system, central banks started to investigate the technology. From the industry side, over one hundred corporations have joined blockchain working groups or consortia and the number of patents filled increased to more than three thousand in 2017 [5].

Blockchain itself cannot handle large amount of information, because the main purpose is to store simple transactional logs. As a result, scalability of blockchain is a concern for the developers [4]. Even though the technology has been around for a while, there are only a few academic blockchain-related studies. Most of the available non-scientific papers about blockchain technology are whitepapers, documentations or technical documents; some of which may be incomplete or are still being updated. A practical approach to blockchain development also demands considerable investment [6]. Developers need to have a clear understanding of the capabilities and limitations of blockchain technology. Additionally, they need to acquire the necessary skills to implement the technology and to figure out how the new trust architecture would affect the application.

Currently, the blockchain technology is most broadly applied for cryptocurrencies, but other areas are in early adoption as well. Solutions for automating the insurance process [7], supply chain management [8] even some proposals for scientific reproducibility or decentralization of scientific data exist [9] [10]. But various authors describe the same concepts differently and only a few define their development process [8] [11] [12]. The capability for replicating blockchain technology solutions is low, as it is highly dependent on the authors' environment. No formal methods exist, and common elements are difficult to find or to associate. This is particularly noticeable with the more complex elements that support more complicated scenarios [13]. The common process for development of blockchain-based system could ease the applicability in other areas than the financial sector and bridge the knowledge gap among stakeholders of blockchain technology.

Modelling is a common tool for facilitating communication, visualizing the development process and even automating the implementation of some development artefacts. The strategies of Model Driven Development [14] are often applicable in the area of software engineering. Model Driven Architecture (MDA) is a methodology, which encompasses a set of guidelines for specifying models during software development process [15]. Each MDA-based specification has three levels: A Computation Independent Model (CIM), a Platform-Independent Model (PIM), and one or more Platform-Specific Models (PSM). Unified Modelling Language (UML) [16] is commonly used for MDA model development. MDA models can represent system at different levels of abstraction, from various viewpoints, from enterprise architectures to technology implementations [17]. Model-Driven Architecture principles could be adapted to blockchain and smart contract domain together with guidelines for developing blockchain structure and smart contract behavior.

In this paper we present our idea of blockchain technology development method, based on MDA principles. The proposed method could be used for different processes for the definition of common elements and the identification of potential application areas. The method could provide a more structured approach for the development of blockchain elements, which could potentially shorten the time of development. In the future we plan on developing the method further.

The rest of the paper is organized as follows. The second section discusses the background of blockchain technology and its evolution. The third section presents current areas of blockchain application and research on improving blockchain-based systems development process. The fourth section describes our proposition on applying principles of model-driven architecture for blockchain system development. The last section summarizes concludes our main insights and outlines future work.

II. Background

This chapter presents the basic concepts and categories of blockchain technology. In this way, we intend to define the domain in order to outline a common understanding of these technologies and attain a more comprehensive communication in this area. Although the terms "blockchain" and "distributed ledger" are used interchangeably, the blockchain is a type of distributed ledger technology and blockchain mostly differs from distributed ledger in the way the data is stored [5]. For this reason, we refer to these technologies using the terms "blockchain" and "blockchain technologies" as they cover both concepts.

A. Blockchain technology

Blockchain is a distributed database that is shared across participants [18]. Participants can independently verify information because copies of records are available in the blockchain. If a node fails, the remaining ones can continue to operate. Verification process does not depend on a centralized authority. Information is kept in a digital ledger. The transactions in the blockchain are recorded near real time. Once transactions are included in the ledger it is nearly impossible to delete or rollback the changes. Each block is timestamped, and each block has a pointer referring to the data stored in the previous block in the chain.

The data in blocks are hash sealed. The participants can interact with the blockchain only by using a generated address so that the identity of the user is not revealed. Any transaction refers to some previous transactions. Once the current transaction is recorded into the blockchain, the state of referred transactions change. That way transactions can be tracked and verified once needed.

Participants in the network authenticate and approve transactions before inclusion to the blockchain. Few different methods for reaching consensus exist. Consensus algorithms in blockchain are used to maintain data consistency in a distributed network. Usually, the basis of such algorithms is that the majority of network participants needs to approve the correctness of transaction. This way the need for a third party is avoided. In a traditional centralized transaction system, each transaction needs to be validated by a central trusted agency (e.g., the central bank).

The blockchain technologies are divided into three generations, based on the complexity of the components. The first generation of blockchain was all about cryptocurrency and its exchange possibilities. The 2.0 generation focuses heavily on the use of smart contracts built using scripting language of the blockchain. The third generation of blockchain supports decentralized applications based on blockchain technologies in other previously unsupported areas like government, health, science and culture.

1) Blockchain 1.0: Bitcoin and cryptocurrency

Blockchain technology began with Bitcoin, and many developers around the world still consider that the main blockchain example. Blockchain technology relies on a shared public ledger that entire cryptocurrency networks share and depend on. Traditional currency system participants rely on the bank to authenticate the integrity of a ledger, but blockchain relies on peer-to-peer network transfer thus eliminating the need of the third parties. Today, the first generation of blockchain technologies is mainly defined by cryptocurrencies like Bitcoin [19]. Bitcoin has proven to be an effective decentralized digital currency. The relative simplicity of Bitcoin and its inability to handle contracts limits its ability to serve a wider range of use cases.

2) Blockchain 2.0: Ethereum and smart contracts

Bitcoin introduced a very basic scripting language, that allowed some form of contractual complexity. The extension of this scripting language to handle more complex data manipulations within blockchain came to be defined as a second-generation blockchain technology. The second generation is mainly represented by Ethereum. Ethereum proposed a structure in which blockchain technology could be used to facilitate the management of digital assets. Ethereum offers new functionality through so-called smart contracts, which can manage agreements between parties on the blockchain [20]. A smart contract can manage itself, events can be triggered without the need of any party input. Second-generation blockchains can leverage distributed network for computing power, this way smart contracts can execute complicated logic. In such cases, parties do not need to pay a 'trusted' third party and could leave agreements to execute autonomously.

Unfortunately, these blockchain technologies are known to struggle with scaling difficulties. Additionally, neither Ethereum nor Bitcoin is fundamentally integrable with other decentralized currencies or platforms; meaning that in most cases users wishing to transfer value from one platform into another must do so through via exchange services [21].

3) Blockchain 3.0

The new generation blockchains come into existence with a focus to address the issues in both Blockchain 1.0 and 2.0 via different protocols, techniques and frameworks. High scalability, interoperability, adaptability, sustainability, privacy as well as instantaneous transactions are features that should separate Blockchain 3.0 from its previous iterations [19] [22]. The third generation of blockchain is at the time being developed and there are no specific blockchain solutions which define this generation. A candidate for flagship blockchain example in this category should address present flaws of existing solutions.

B. Smart Contracts

An additional implementation of more advanced data manipulation mechanism for blockchain enabled application layer development in the form of smart contracts. Basically, a smart contract is a deployed program that can be executed on the blockchain network following the principle of trigger causing an appropriate reaction [23] [24]. Smart contracts can express triggers, conditions, and even cover entire business processes [11]. A contract can be viewed as a simple class, or it can contain complex structures, functions, modifiers, events for the implementation of various level of logic [25]. Usually, blockchains have a built-in scripting language, which is used to execute additional business logic triggered by a transaction. Recent generations of blockchains (e.g. Ethereum and Hyperledger) use integrated programming language executable by a virtual machine [2].

The consumer deals directly with the transactions on the blockchain, a smart contract holds value which is released at the time certain conditions are met, this way the contracts have lower transactional costs unlike traditional contracts [12]. Smart contracts could theoretically cover entire software applications, but most smart contracts currently are like traditional contracts for creating legally binding agreements between certain parties. Other areas of applications for smart contract hold entertainment value (e.g. CryptoKitties [26]), unlike aforementioned contracts, these contracts are most likely developed by people with interest in Solidity (contract-oriented programming language for writing smart contracts on Ethereum blockchain) [11]. Smart contract code generation would potentially simplify the smart contract development process, raise the abstraction level and increase potential usage in various domains.

Blockchain technologies are rapidly evolving and the area of their application broadens. Our research focusses on analyzing the applicability of these technologies in various areas and possibilities of improving the development process of blockchain-based systems.

III. RELATED WORK

In this section we overview applications of blockchain technologies in various fields and discuss difficulties of application of blockchain technology to diverse domains. The research on the applicability of modelling techniques to blockchain-based system development is also overviewed.

One of the blockchain application areas is tracking the provenance of assets. Solutions like supply chain management are one of the business issues that could benefit from automation with smart contracts. Evaluation of provenance is generally difficult not only because of the number of goods that are handled in complex supply chains but also because of the amount of information for tracking product location, physical characteristics. As a solution to this problem, simple data models of the ontology were described. These models were later used to develop smart contract implementation [8].

Another way to utilize smart contract on blockchain is insurance-related contracts. The extended solution in a form of framework exists to help developers deploy more secure and less costly contracts. Smart contracts can automate the processes of insurance operations such as client registration, policy assignment, premium payouts, submission claims, and processing of refunds without or with minimal involvement of third parties [7].

As well as business processes, there are many suggestions to improve scientific processes using blockchain technologies [9] [10]. Proposals for implementing blockchain technologies could be grouped into three groups: the first that uses blockchain as a storage unit or as a token indicating possession and the second that proposes using blockchain to work on scientific computations giving monetary rewards or free of charge. There are suggestions for blockchain to be used as a platform to store medical data [27]. Storing medical data in blockchain makes medical data more accessible for medical staff and general public alike. Also, there are propositions to use blockchain technology as a proof of intellectual work [10]. This could enable scientists or members of the general public to store ideas in the blockchain with a timestamp of the proposed idea. The second category is run by business and scientific organizations alike [28] [29]. The third category uses blockchain technologies for both storing data and performing computational tasks. An example of the third category could be blockchain used for federated learning and also analyzed the latency aspects of their proposed architecture [30].

Blockchain use cases continue to grow in scope and complexity, that is why the need for common guidelines becomes apparent [31]. For blockchain to be accepted as a technology in other industries besides financial, it is essential that stakeholders have a common understanding of the technology and possibilities of blockchain [32]. A few proposals for standardization of software engineering of blockchain technologies have emerged during the last year [11] [33] [34] [35]. The author of [11] proposes a development method which includes smart contract development approach based on MDA. In [33] a general proposal is presented for extending existing modelling notations to include specific blockchain concepts or integrations. An approach for the modelling blockchain business networks via layer-based modeling and ontology design is presented in [34]. Authors describe abstraction layer which can be used to describe blockchain and develop a Blockchain Business Network Ontology which depicts common terms for blockchain networks. A model-driven approach for generation of smart contract code of is described in [35]. Authors develop BPMN process model for collaborative business process and use it for generation of smart contract code. In the area of information systems, the application of blockchain technology and cryptocurrencies is still quite limited [2] [5]. In order to adapt blockchain technology to specific needs, the main attention should be paid to the development and implementation methodologies of such technologies.

The lack of a formal and unified methodology complicates the application of blockchain technology. Only a small portion of authors describe their development process, unfortunately these are often specialized for specific use cases. A universal method for development could ease the design and implementation process of blockchain technology-based systems [36]. Introduction of some standard way for defining and specifying blockchain structure and behavior could facilitate the blockchain development process [37]. There are proposals suggesting that blockchain components could be modeled using BPMN and UML [33], although researchers are not proposing to apply MDA to the whole development process. A similar proposal of using modelling to define smart contracts have been proposed in [38]. An approach to Ethereum smart contract development was also proposed [11]. The analyzed proposals for modelling of blockchain and smart contracts are in the early stages and have not yet been extensively validated or tested.

Based on the analysis of blockchain application areas and proposed techniques for its implementation, introduction of a common methodology for blockchain-based system development could facilitate the development process and broaden the scope of its applications.

IV. Applying the Principles of Model-Driven Architecture for Blockchain-Based Systems Development

To facilitate the development of a blockchain-based system, we propose a methodology based on MDA principles. We believe, that such methodology could help to describe blockchain-based systems concepts and behavior in a more general language [37]. Furthermore, some development actions could be accelerated by automation. This methodology is seen as covering five system development stages (Fig. 1). For each stage, a certain type of resource required and a certain set of outcomes is identified. UML and its extension in a form of UML profile for blockchain specified using domain specific language (DSL) [39] are proposed as a language for modelling different aspects of the system. Below the methodology is explained in more detail.

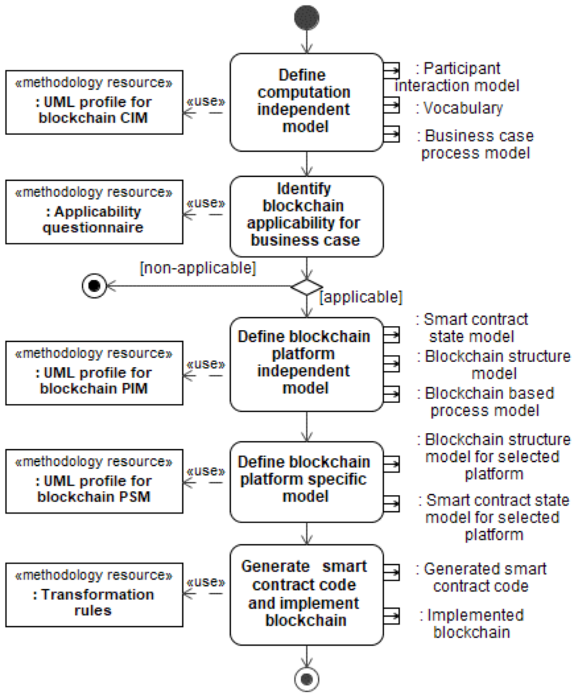
«methodology resource»
: UML profile for blockchain CIM
«use»
Define computation independent model
: Participant interaction model
: Vocabulary
: Business case process model
«methodology resource»
: Applicability questionnaire
«use»
Identify blockchain applicability for business case
[non-applicable]
[applicable]
«methodology resource»
: UML profile for blockchain PIM
«use»
Define blockchain platform independent model
: Smart contract state model
: Blockchain structure model
: Blockchain based process model
«methodology resource»
: UML profile for blockchain PSM
«use»
Define blockchain platform specific model
: Blockchain structure model for selected platform
: Smart contract state model for selected platform
«methodology resource»
: Transformation rules
«use»
Generate smart contract code and implement blockchain
: Generated smart contract code
: Implemented blockchain

Fig. 1. The proposed process for blockchain-based business process implementation

In the first development stage Computation Independent Model (CIM) should be specified. The purpose of this model is to show how blockchain could be adapted for specific processes' restructuring, reorganization, and integration. In MDA, a Computation Independent Model (CIM) is often referred to as a business or domain model. It presents the context of the system under development and what the system is expected to do but hides all information technology related specifications to remain independent. A model should be created using the provided UML profile for blockchain CIM. It would consist of a participation interaction model, vocabulary and a business case process model.

Due to the fact that blockchain technology is not applicable in every case, solutions helping to determine the suitability of blockchain exists [40]. These questions/frameworks help to assess the advantages and limitations of blockchain technology and the applicability of the technology for general purposes. Following this example, the second step of the method would be to identify whether blockchain is applicable in the specific case. Using the defined CIM and applicability questionnaire the specific case would be assessed, and the outcome would be the conclusion whether to proceed with the development of blockchain.

If blockchain technology is applicable, the development of the blockchain would continue with the design of the Platform Independent Model (PIM). Traditionally PIM represents the design of the system without the details about its implementation. Considering the method is tailored for the blockchain, the defined models would include details about implementation, but would not be based on any specific blockchain technology (e.g. Hyperledger or Ethereum). The previously described CIM models would be used as an input for the development of the PIM. Using the blockchain PIM, a smart contract state model, blockchain structure model and blockchain-based process model can be defined. These defined models would help to select a specific platform for further development because different platforms differ in terms of chain architecture, transaction structure, number of participants, smart contract capabilities, consensus algorithms and so on.

Afterwards the development of blockchain Platform Specific Model (PSM) would take place. MDA suggests automating the production of a PSM from previously defined models. It requires to define transformation rules which specify how models are transformed based on parameters defined by developers [15] [17]. The PSM of a system is defined and tailored for a specific platform. In our proposed method a PSM would be developed for a specific blockchain implementation. The previously defined PIM model would be used to define blockchain structure and smart contract model for the selected platform. Specialized model for a particular blockchain solution could be provided in a form of DSL. Finally, in the last stage applying transformation rules for the specific blockchain PSM model the code for smart contract and blockchain implementation of that particular platform would be generated. The generated artefacts could be used to start building specific blockchain technology implementation.

The proposed methodology would not only help to define the blockchain artefacts, but also help to identify whether it is reasonable to adopt the technology. It could also offer guidelines for selecting appropriate blockchain platform. The solution would provide the possibility to facilitate and at least partially automate the blockchain technology-based system development process by providing a more standardized way of describing such systems, expanding the potential uses of blockchain for different business goals by restructuring current business processes.

V. Conclusion

The blockchain technologies are currently most broadly applied in the financial sector, and the application in other areas is still quite limited. The design process of blockchain technology-based systems is quite difficult, because no formal or formalized design, development methodologies exist. A proposed application of MDA principles in the process of development of blockchain technology-based systems should help to determine whether it is possible to model blockchain structure and smart contract logic and whether the business logic could be conveyed in the smart contracts. The methodology could be used for modelling blockchain and smart contracts of business processes and thus relocating these to the blockchain. In addition, an extensive analysis of business processes is still required for determining how the relocation of the business logic to the blockchain could affect the current processes. Going forward, it is essential to thoroughly examine the possibilities of adopting MDA principles for blockchain technology-based system development process. It is important to analyze blockchain implementations and find common elements. The results should help to determine how to model blockchain structure and smart contract logic, and how business logic can be conveyed by the smart contracts.

References

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf .

[2] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis," in Proceedings of the 50th Hawaii International Conference on System Sciences , 2017.

[3] M. Swan, Blockchain Blueprint for a New Economy, O'Reilly Media, 2015.

[4] S. Raval, Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, O'Reilly Media, 2016.

[5] P. Tasca and C. J. Tessone, "Taxonomy of Blockchain Technologies. Principles of Identication and Classication," 2018. [Online]. Available: https://dx.doi.org/10.2139/ssrn.2977811.

[6] D. W. Cearley, B. Burke, S. Searle and M. J. Walker, "Top 10 Strategic Technology Trends for 2018," Garnter, 2017.

[7] M. Raikwar, S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay and K.-Y. Lam, "A Blockchain Framework for Insurance Processes," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.

[8] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," Intelligent Systems in Accounting, Finance and Management, 28 March 2018.

[9] b8d5ad9d974a44e7e2882f986467f4d3, "Towards Open Science: The Case for a Decentralized Autonomous Academic Endorsement System," 12 4 2016. [Online]. Available: 10.5281/zenodo.60054.

[10] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in Learning: Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, 2016.

[11] K. Boogaard, A Model-Driven Approach to Smart Contract Development, 2018.

[12] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application," 2014. [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[13] D. Furlonger and R. Valdes, "Practical Blockchain: A Gartner Trend Insight Report," Gartner, 2017.

[14] O. Pastor, S. España, J. I. Panach and N. Aquino, "Model-Driven Development," Informatik Spektrum , 2008.

[15] O. Pastor and J. C. Molina, Model-Driven Architecture in Practice, Springer, 2007.

[16] O. M. Group, "UML 2.5 Specification," 01 03 2015. [Online]. Available: http://www.omg.org/spec/UML/2.5/PDF.

[17] Object Management Group, "Model Driven Architecture (MDA) MDA Guide rev. 2.0," 18 June 2014. [Online]. Available: https://www.omg.org/cgi-bin/doc?ormsc/14-06-01.

[18] Deloitte, "Blockchain @ Media | A new Game Changer for the Media Industry?," 2017 . [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/deloitte-PoV-blockchain-media.pdf.

[19] B. Smith, "What are the three generations of blockchain, and how are they similar to the web?," 2018. [Online]. Available: https://www.coininsider.com/three-generations-of-blockchain/.

[20] G. Wood, "Ethereum: a Secure Decentralised Generalised Transaction Ledger," 2014. [Online]. Available: https://gavwood.com/paper.pdf.

[21] B. Smith, "The blockchain can succeed like the web – here's how," Coin Insider, 18 December 2018. [Online]. Available: https://www.coininsider.com/the-blockchain-can-succeed-like-the-web-heres-how/.

[22] "What is Blockchain Technology?," 2018. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/.

[23] M. Vincenzo, Business Innovation Through Blockchain: The B3 Perspective, 2017, p. 101–124.

[24] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," AI Matters, vol. 1, no. 2, pp. 19-21, 2014.

[25] N. Prusty, Building Blockchain Projects, Packt Publishing, 2017.

[26] U. W. Chohan, The Leisures of Blockchains: Exploratory Analysis, SSRN, 2017.

[27] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in International Conference on Open and Big Data, Vienna, 2016.

[28] J. Zawistowski, P. Janiuk, A. Regulski and A. Skrzypczak, "The Golem Project," 2016. [Online]. Available: https://golem.network/crowdfunding/Golemwhitepaper.pdf.

[29] G. Fedak, W. Bendella and E. Alves, "Blockchain-Based Decentralized Cloud Computing," 2018. [Online]. Available: https://iex.ec/wp-content/uploads/pdf/iExec-WPv3.0-English.pdf.

[30] H. Kim, J. Park, M. Bennis and S.-L. Kim, "On-Device Federated Learning via Blockchain and its Latency Analysis," CoRR, 2018.

[31] E. Piscini, D. Dalal, D. Mapgaonkar and P. Santhana, "Blockchain to blockchains," in Tech Trends 2018: The symphonic enterprise, 2017.

[32] J. d. Kruijff and H. Weigand, "Understanding the Blockchain Using Enterprise Ontology," 2017. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-59536-8_3.

[33] H. Rocha and S. Ducasse, "Preliminary Steps Towards Modeling Blockchain Oriented Software," in 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, 2018.

[34] S. Seebacher and M. Maleshkova, "A Model-driven Approach for the Description of Blockchain Business Networks," in Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.

[35] X. Xu, I. Weber and M. Staples, "Model-Driven Engineering for Blockchain Applications," in Architecture for Blockchain Applications , Springer, 2019, pp. 149-172.

[36] C.-F. Liao, S.-W. Bao, C.-J. Cheng and a. K. Chen, "On Design Issues and Architectural Styles for Blockchain-driven IoT Services," in IEEE International Conference on Consumer Electronics , Taiwan, 2017.

[37] A. B. Tran, X. Xu, I. Weber, M. Staples and P. Rimba, "Regerator: a Registry Generator for Blockchain," in CaiSE2017: 29th International Conference on Advanced, Essen, Germany, 2017.

[38] M. Marchesi, L. Marchesi and R. Tonelli, "An Agile Software Engineering Method to Design Blockchain Applications," in Software Engineering Conference Russia, Moscow, 2018.

[39] A. V. Deursen, E. . Visser and J. . Warmer, "Model-Driven Software Evolution: A Research Agenda," , 2007. [Online]. Available: http://swerl.tudelft.nl/twiki/pub/eelcovisser/modeldrivensoftwareevolutionaresearchagenda/dvw07.pdf. [Accessed 30 1 2019].

[40] Kapuściński, T., Nowicki, R. K., & Napoli, C. (2016, June). Application of genetic algorithms in the construction of invertible substitution boxes. In International Conference on Artificial Intelligence and Soft Computing. Springer, Cham, p. 380-391.

[41] K. Wüst and A. Gervais, "Do you need a Blockchain?," 2017.