Catchword: Blockchains and Enterprise Modeling

Hans-Georg Fill[*,a], Peter Fettke[b], Stefanie Rinderle-Ma[c]

[a] University of Fribourg, Switzerland
[b] Saarland University and German Research Center for Artificial Intelligence (DFKI), Germany
[c] University of Vienna, Austria

Abstract. *In this catchword article we describe the current technological opportunities that are available through blockchain technologies and outline how the field of enterprise modeling can contribute to these developments as well as benefit itself from them. For this purpose, we discuss the technical foundations of blockchains and derive a framework for relating both sides. Finally, it is reported about recent approaches that already engage in these opportunities.*

Communicated by Agnes Koschmider. Received 2020-12-09. Accepted on 2020-12-11.

1 Introduction

Over the last years, blockchains and more generally distributed ledger technologies (DLT) received the attention of many stakeholders. This was due on the one hand to the rise of Bitcoin as a successful proof-of-concept for a reliable cryptocurrency that eliminated the need for central banks to guarantee for value and permit the decentralized, immutable, and secure transfer of monetary assets between parties (Reinhard 2019). On the other hand, the underlying technologies were considered as fundamental game changers with the potential to not only disrupt the financial sector but extend to many other industries (Iansiti and Lakhani 2017). Apart from this hype and the disappointment that followed it, researchers in academia and industry were and are still attracted by the new possibilities that are offered by decentralized and transparent systems, which do not require any central authority for validating transactions (Dabbagh et al. 2019; Al-Jaroodi and Mohamed 2019; Lacity and Khan 2019). Most recently, several of the big IT platform companies such as Amazon (Amazon.com 2019), Microsoft (Simons 2019), IBM (Cuomo 2019) or Facebook (Zuckerberg 2019) started to engage heavily in blockchain-based approaches.

1.1 Core Properties of Blockchains

At the current stage it is thus being investigated, how scenarios in enterprise information systems can be realized with these new technologies. This is based on the following core properties of blockchains (Antonopoulos and Wood 2018; Fill and Meier 2020; Narayanan et al. 2016):

- Decentralized storage of data
- Trustful validation of data via consensus mechanisms
- Transparency and traceability of transactions
- Immutability and non-repudiation of transactions
- Decentralized execution of algorithms using smart contracts

In contrast to traditional web-based information systems, data in blockchains is not held and governed by a central authority. Rather, all participants of the ledger have access to the complete data set and can verify its contents individually. The addition of data is accomplished through validations executed by any of the participants and the use of consensus mechanisms for reaching a

* Corresponding author.
E-mail. hans-georg.fill@unifr.ch

common agreement about the new state of the blockchain. This leads to the transparency and traceability of transactions, not only for the owner of the system as in traditional systems but for every participant. Consequently, a new form of trust is established as everything that happens on the ledger is transparent and verifiable.

Another core feature of blockchains is the immutable storage of information and thus the non-repudiation of transactions. This means that such ledgers are append-only and all transactions are cryptographically signed by the issuers of transactions. This aspect is of particular importance for public blockchains to guarantee the traceability of all transactions. For private or permissioned blockchains where the participants are authenticated prior to their interaction with the blockchain, this can be altered, e. g. to permit for the secure transmission of information in separate channels as in Hyperledger Fabric[1] for example.

Although all blockchain implementations use a set of operation codes for specifying how transactions are actually performed, some platforms such as Ethereum (Antonopoulos and Wood 2018), Hyperledger Fabric (Hyperledger 2019) or Libra (Blackshear et al. 2019) provide more comprehensive commands. Thereby, Turing-complete programs can be described and integrated in the ledger. These are typically denoted as *smart contracts* and enable the realization of functionality such as automated payments due to state changes in the blockchain, the recording of and access to arbitrary types of data on the blockchain, or the interaction with external systems. As for any transaction on a blockchain, also the execution and state changes caused by smart contracts are decentralized, transparent, and verifiable by any participant.

1.2 Role of Enterprise Modeling

Enterprise modeling is typically regarded as a sub-area of conceptual modeling with a specific focus on enterprise information systems (Bork and Fill 2014; Frank 2014). Conceptual modeling thereby refers to the use of a schema in the form of an artificial language together with procedures and algorithms for creating models, which determine the construction and contents of models (Karagiannis and Kuehn 2002; Mylopoulos 1992). Depending on the purpose of the conceptual models, the schema may come in the form of a general-purpose modeling language (GPML) that provides generic language constructs or a domain-specific modeling language (DSML) that provides constructs that have been designed for a particular domain. Moreover, the language may be formally specified, i. e. in terms of a precise mathematical specification of its syntax and semantics, or of semi-formal nature where only the syntax is formally defined and the semantics given in natural language (Fraser et al. 1994; Harel and Rumpe 2004).

Models themselves are used in all scientific disciplines and can be characterized in this context as constructed abstractions that aim at reducing complexity for the purpose of human understanding and communication (Frank et al. 2014; Mylopoulos 1992). Due to the formalization of conceptual models via their schema, algorithms may be designed that are able to interpret the semantics of the models' contents (Harel and Rumpe 2004). This not only permits the processing of the contents, e. g. using simulation algorithms, but also the execution of models in the sense of deriving operation codes for machines.

In enterprise information systems, conceptual models are not only used for representing and analyzing technical aspects as it is primarily done in computer science. Rather, the purpose of enterprise models is to provide an integrated representation of strategies, processes, IT services and applications, and infrastructures (Ferstl and Sinz 1998; Frank 2014; The Open Group 2017). Enterprise modeling is today a standard practice for tasks such as (Sandkuhl et al. 2018):

- Eliciting requirements for information systems based on the knowledge of stakeholders, e. g. in

[1] See https://hyperledger-fabric.readthedocs.io/en/release-1.4/channels.html

terms of goals, processes, IT services, performance indicators,

- Implementing and deploying information systems, e. g. in software engineering and enterprise architecture management,
- Analyzing information systems, e. g. for business process simulation and improvement,
- Operating information systems, e. g. via the execution of models on process engines.

Based on these aspects it seems obvious to investigate how blockchains and enterprise models can complement each other. We will do this in the following by first outlining some further technical details on blockchains. Subsequently, we will derive a framework for depicting possible relationships between enterprise models and blockchains from various perspectives. This will permit us to position existing approaches reverting to blockchains in enterprise modeling and illustrate opportunities for further research.

2 Technical Foundations of Blockchains

For understanding the working of blockchains it is essential to know about the typical underlying data structure and the mechanisms that lead to the immutability of transactions and the achievement of distributed consensus without intermediaries. In the following we will thus briefly illustrate these aspects. Thereby we revert mainly to the architecture of Bitcoin, which is one of the most widely, working implementations of blockchains. Although no official specification exists for Bitcoin and the way it works is only available at first hand from its concrete implementation, i. e. the code base, we revert here primarily to the documentation maintained by the community (Bitcoin Community 2019a).

One essential concept that is used for building data structures in blockchains are cryptographic hash functions (Handschuh 2011; Narayanan et al. 2016). Hash functions in general take an input of arbitrary size and map it to a specific output of fixed size. Depending on the size of the output, the probability of collisions, i. e. where the same output value is produced for different inputs, can be adjusted. Cryptographic hash functions feature the two additional properties *collision resistance* and *pre-image resistance*. Collision resistance means that it is computationally infeasible to find two input values that produce the same output value. Pre-image resistance demands that the hash function is a one-way function, i. e. that the input value cannot be computed easily from the output value. In addition, blockchains make use of digital signatures (Narayanan et al. 2016). For this purpose, it is reverted to public key cryptography where a message is encrypted with the public key of the receiver and decrypted with the corresponding private key that is securely held by the receiver. For signing messages, this process is reversed in that the sender signs the message by encrypting a hash value of the message using her private key. The authenticity of the message can then be verified by using the public key of the sender for decrypting the message and comparing the hash value to the re-calculated hash value of the message.

Cryptographic hash functions and digital signatures form the basis for the typical data structures used in blockchains. As depicted in Figure 1, a data block in a blockchain like Bitcoin consists of a magic number for separating blocks from each other by a pre-defined value, a number for the size of the block, transactions and the number of transactions as meta data, and the block header. The transactions are cryptographically signed and define how value or assets are transferred in the blockchain or how code is executed in the case of smart contracts.

The block header defines the version of the currently used protocol and contains a reference to the header of the previous block in the form of a hash value. Furthermore, a timestamp and a root-hash of a Merkle tree summarizing the contained transactions is included.

In addition, public blockchains such as Bitcoin use consensus mechanisms where so-called *cryptographic puzzles* have to be solved in order to

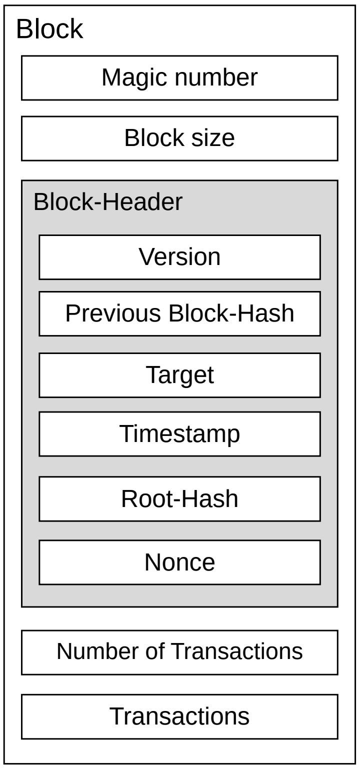

Figure 1: Structure of Blocks as Used in Bitcoin, cf. (Bitcoin Community 2019b)

realize a lottery-like selection of blockchain participants for adding the next block. For this purpose, a hash value is calculated from the concatenation of the version field, the previous block-hash, the root-hash, the timestamp, a target field and a nonce field. The target field thereby specifies an upper-bound value for the resulting hash value. For a blockchain participant to be chosen as the next proposer of a block to be appended to the blockchain, a hash value has to be found that lies below this target value. The variation is thereby accomplished through the nonce field, which stands for *number-used-only-once*. This is an arbitrary number that is varied as long as the target hash value range is not reached. For finding such a nonce, computational work has to be performed and no shortcuts are possible due to the above-described properties of the used cryptographic hash functions. Therefore, this type of consensus mechanism is denoted as *proof-of-work*. Other mechanisms exist but have not proven their success in practice yet.

When a solution to this puzzle has been found, the block including the matching nonce is distributed to other peers in the network. These can easily verify the correctness of the puzzle solution by calculating the hash value and comparing it to the target value. If this is valid, the block is appended to the blockchain. In the case of competing block proposals, i. e. when several participants have found solutions at the same time, the chain with the most proven work, i. e. typically the longest chain, is maintained. The other chains are given up and no longer followed. To account for changes in the available computational power, the target is automatically adjusted after a certain number of blocks to keep the time of finding a new solution constant, which is also checked when blocks are validated by the peers.

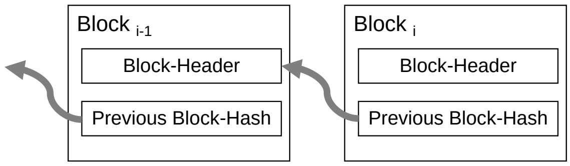

Figure 2: Chaining of Blocks

This mechanism permits every participant of the blockchain to independently engage in the selection process for proposing new blocks to the blockchain without requiring a central intermediary. The reference to the hash value of the block header of the previous block thereby forms the chain structure as shown in Figure 2.

Blockchains are not the only type of distributed ledger technologies. Another proposal that is currently being evaluated is the use of data structures based on directed acyclic graphs (DAG). Thereby, new blocks have to validate two other previous blocks and there is no single chain to which blocks are appended. An implementation is for example available by the IOTA approach in the form of so-called *tangles* (Popov 2018).

3 Blockchains and Enterprise Modeling

When combining the fields of blockchains and enterprise modeling, we can find two directions:

1. Enterprise modeling for blockchain applications
2. Integration of blockchain technologies in modeling applications

The first direction takes the traditional view of enterprise modeling for supporting the development of new and the analysis of existing applications. Thereby, blockchains are regarded as a technology that needs to be added to the existing stack of technologies in an enterprise and which may open up new opportunities on the level of strategies and business models, business processes, IT services and the management of IT infrastructure. Thereby, the specific aspects of blockchains, such as for example the possibility of decentralized autonomous organizations have to be considered. In Figure 3, this is denoted by the integration of blockchains on the level of strategy BC_S, processes BC_P, IT services and applications BC_{IS} and infrastructure BC_{IN}.

This direction is pursued e. g. for the following purposes:

- for explaining the business and technological aspects of blockchains by using general-purpose and domain-specific modeling languages (Fill 2020; Wieland and Fill 2020)
- for blockchain-oriented software development by using extended UML class diagrams in addition to BPMN and ER diagrams (Rocha and Ducasse 2018)
- for the visual design and analysis of blockchain-based applications (Härer and Fill 2019a), e. g. by analyzing blockchain applications using Petri nets (Pinna et al. 2018)

The second direction integrates blockchain technologies in enterprise modeling applications. In this way, the properties of blockchains are joined with the properties of enterprise models, e. g. for storing or executing the models. In Figure 3 this is denoted by the area BC_G.

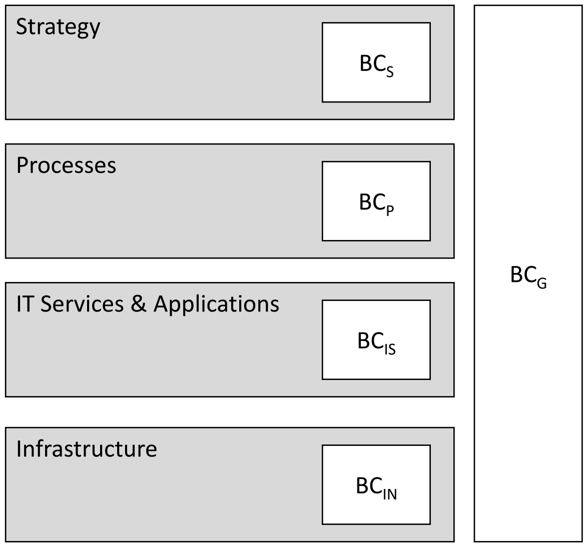

Figure 3: Intersections when Combining the Fields of Enterprise Modeling and Blockchains

This direction is found in the following contributions for example:

- for storing knowledge in the form of enterprise models in a transparent, decentralized, tamperproof way, and for attestation purposes (Fill and Härer 2018; Fill 2019; Härer and Fill 2019b)
- for the execution of business processes in BPMN notation using smart contracts (López-Pintado et al. 2017)
- for the execution of business processes using an adapted notation (Falazi et al. 2019)
- for the execution of decision models in DMN through mapping model constructs to the Solidity language for Ethereum blockchains (Haarmann et al. 2018)
- for tracking of process instances in a distributed fashion (Härer 2018)
- for the storage of models for ensuring the provenance of information in AI applications (Fill and Härer 2020)

4 Conclusion and Outlook

The combination of blockchain technologies and enterprise modeling opens up a lot of opportunities for research. In this catchword we showed which recent advancements have been made. However, there are still several issues that will need to be tackled in the future. This stems on the one hand from the technical evolution of blockchain platforms and on the other hand from the further development of enterprise modeling approaches. In terms of blockchain platforms several limitations currently hamper the successful application in business scenarios. This concerns for example the limitation of the size of blocks in current implementations, which permits to store only comparatively small data on chain. Whereas this does not pose problems for attestation approaches, it does not permit storing for example complete models on current platforms. Further, the processing time in current public blockchain designs does not allow for scalable enterprise applications. Although first approaches exist to combine blockchains and ERP systems (Linke and Strahringer 2020), this is not yet a standard practice. Further research will also need to be done for applying enterprise modeling for designing blockchain-based applications including their business models and enterprise architectures.

References

Amazon.com (2019) Amazon Managed Blockchain https://aws.amazon.com/managed-blockchain/?nc1=h_ls

Antonopoulos A. M., Wood G. (2018) Mastering ethereum: building smart contracts and dapps. O'Reilly Media

Bitcoin Community (2019a) Bitcoin Wiki https://en.bitcoin.it/wiki/Main_Page

Bitcoin Community (2019b) Bitcoin Wiki - Block Structure https://en.bitcoin.it/wiki/Block

Blackshear S., Cheng E., Dill D. L., Gao V., Maurer B., Nowacki T., andShaz Qadeer A. P., Rain, Russi D., Sezer S., Zakian T., Zhou R. (2019) Move: A Language With Programmable Resources https://developers.libra.org/docs/assets/papers/libra-move-a-language-with-programmable-resources.pdf

Bork D., Fill H.-G. (2014) Formal Aspects of Enterprise Modeling Methods: A Comparison Framework. In: 47th Hawaii International Conference on System Sciences. IEEE, pp. 3400–3409

Cuomo J. (2019) Introducing the next-gen platform for enterprise blockchain https://www.ibm.com/blogs/blockchain/2019/06/introducing-the-next-gen-platform-for-enterprise-blockchain/

Dabbagh M., Sookhak M., Safa N. S. (2019) The Evolution of Blockchain: A Bibliometric Study. In: IEEE Access 7, pp. 19212–19221

Falazi G., Hahn M., Breitenbücher U., Leymann F. (2019) Modeling and execution of blockchain-aware business processes. In: Computer Science - R&D 34(2-3), pp. 105–116

Ferstl O. K., Sinz E. J. (1998) SOM Modeling of Business Systems In: Handbook on Architectures of Information Systems Springer, pp. 339–358

Fill H.-G., Härer F. (2018) Knowledge Blockchains: Applying Blockchain Technologies to Enterprise Modeling. In: Hawaii International Conference on System Sciences 2018 (HICSS-51). AIS, pp. 4045–4054

Fill H.-G. (2019) Applying the Concept of Knowledge Blockchains to Ontologies. In: Proceedings of the AAAI 2019 Spring Symposium on Combining Machine Learning with Knowledge Engineering (AAAI-MAKE 2019). CEUR Workshop Proceedings. Vol. 2350. CEUR-WS.org

Fill H.-G. (2020) Enterprise Modeling: From Digital Transformation to Digital Ubiquity. In: 2020 15th Conference on Computer Science and Information Systems (FedCSIS). IEEE, pp. 1–4

Fill H.-G., Härer F. (2020) Supporting Trust in Hybrid Intelligence Systems Using Blockchains. In: Proceedings of the AAAI 2020 Spring Symposium on Combining Machine Learning and Knowledge Engineering in Practice (AAAI-MAKE 2020). CEUR Workshop Proceedings. Vol. 2600. CEUR-WS.org

Fill H.-G., Meier A. (2020) Blockchain kompakt. Springer

Frank U. (2014) Multi-perspective enterprise modeling: foundational concepts, prospects and future research challenges. In: Software and Systems Modeling 13(3), pp. 941–962

Frank U., Strecker S., Fettke P., vom Brocke J., Becker J., Sinz E. (2014) The Research Field “Modeling Business Information Systems”. In: Business & Information Systems Engineering 6(1), pp. 39–43

Fraser M., Kumar K., Vaishnavi V. (1994) Strategies for incorporating formal specifications in software development. In: Communications of the ACM 37(10), pp. 74–86

Haarmann S., Batoulis K., Nikaj A., Weske M. (2018) DMN Decision Execution on the Ethereum Blockchain. In: International Conference on Advanced Information Systems Engineering (CAiSE 2018). Lecture Notes in Computer Science. Vol. 10816. Springer, pp. 327–341

Handschuh H. (2011) SHA-0, SHA-1, SHA-2 (Secure Hash Algorithm) In: Encyclopedia of Cryptography and Security. Springer, pp. 1190–1193

Harel D., Rumpe B. (2004) Meaningful Modeling: What’s the Semantics of "Semantics"? In: IEEE Computer 37(10), pp. 64–72

Härer F. (2018) Decentralized Business Process Modeling and Instance Tracking Secured By a Blockchain. In: European Conference on Information Systems. Research Papers. Vol. 55. AIS, pp. 1–17

Härer F., Fill H.-G. (2019a) A Comparison of Approaches for Visualizing Blockchains and Smart Contracts. In: Jusletter IT 2019(1)

Härer F., Fill H.-G. (2019b) Decentralized attestation of conceptual models using the Ethereum blockchain. In: 2019 IEEE 21st Conference on Business Informatics (CBI) Vol. 1. IEEE, pp. 104–113

Hyperledger (2019) Hyperledger Fabric 1.4 Documentation: Smart Contract Processing https://hyperledger-fabric.readthedocs.io/en/release-1.4/developapps/smartcontract.html

Iansiti M., Lakhani K. R. (2017) The truth about blockchain. In: Harvard Business Review 95(1), pp. 118–127

Al-Jaroodi J., Mohamed N. (2019) Blockchain in Industries: A Survey. In: IEEE Access 7, pp. 36500–36515

Karagiannis D., Kuehn H. (2002) Metamodeling Platforms In: International Conference on Electronic Commerce and Web Technologies (EC-Web 2002) Vol. 2455 Lecture Notes in Computer Science. Springer, p. 182

Lacity M., Khan S. (2019) Exploring Preliminary Challenges and Emerging Best Practices in the Use of Enterprise Blockchains Applications. In: Proceedings of the 52nd Hawaii International Conference on System Sciences. University of Hawaii at Manoa, pp. 4665–4674

Linke D., Strahringer S. (2020) Blockchain-Integration in ERP-Systeme–Fallbeispiel Daimler AG. In: Blockchain – Grundlagen, Anwendungsszenarien und Nutzungspotenziale. Springer, pp. 173–193

López-Pintado O., García-Bañuelos L., Dumas M., Weber I. (2017) Caterpillar: A Blockchain-Based Business Process Management System. In: BPM Demo Track and BPM Dissertation Award. CEUR Workshop Proceedings. Vol. 1920. CEUR-WS.org

Mylopoulos J. (1992) Conceptual Modeling and Telos In: Conceptual Modelling, Databases and CASE: An Integrated View of Information Systems Development. Wiley, pp. 49–68

Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016) Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press

Pinna A., Tonelli R., Orru M., Marchesi M. (2018) A Petri Nets Model for Blockchain Analysis. In: The Computer Journal 61(9), pp. 1374–1388

Popov S. (2018) The Tangle https://iota.org/IOTA_Whitepaper.pdf

Reinhard B. (2019) Zehn Jahre Blockchain - Bitcoin, Crypto Kitties und die digitale Blockchain-ID - Eine Reise. In: Wirtschaftsinformatik & Management 11(2), pp. 81–83

Rocha H., Ducasse S. (2018) Preliminary Steps Towards Modeling Blockchain Oriented Software. In: International Workshop on Emerging Trends in Software Engineering for Blockchain. ACM/IEEE, pp. 52–57

Sandkuhl K., Fill H.-G., Hoppenbrouwers S., Krogstie J., Matthes F., Opdahl A., Schwabe G., Uludag Ö., Winter R. (2018) From Expert Discipline to Common Practice: A Vision and Research Agenda for Extending the Reach of Enterprise Modeling. In: Business & Information Systems Engineering 60(1), pp. 69–80

Simons A. (2019) Toward scalable decentralized identifier systems https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Toward-scalable-decentralized-identifier-systems/ba-p/560168

The Open Group (2017) ArchiMate® 3.0.1 Specification http://pubs.opengroup.org/architecture/archimate3-doc/chap03.html#_Toc489945971

Wieland M., Fill H.-G. (2020) A Domain-Specific Modeling Method for Supporting the Generation of Business Plans. In: Modellierung 2020, pp. 45–60

Zuckerberg M. (2019) Libra - A New Global Currency https://www.facebook.com/zuck/posts/10107693323579671