2020

Towards a Blockchain Technology Framework – Literature Review on components in blockchain implementations

Matthias Pohl
Otto-von-Guericke University, matthias.pohl@ovgu.de

Rene Degenkolbe
Otto-von-Guericke University, rene.degenkolbe@ogvu.de

Daniel Staegemann
Otto-von-Guericke University, daniel.staegemann@ovgu.de

Klaus Turowski
Otto-von-Guericke University, klaus.turowski@ovgu.de

Towards a Blockchain Technology Framework – Literature Review on components in blockchain implementations

Completed research paper

Matthias Pohl
Very Large Business Applications Lab
Otto von Guericke University
Magdeburg, Germany
Email: matthias.pohl@ovgu.de

Rene Degenkolbe
Faculty of Informatics
Otto von Guericke University
Magdeburg, Germany
Email: rene.degenkolbe@ovgu.de

Daniel Gunnar Staegemann
Faculty of Informatics
Otto von Guericke University
Magdeburg, Germany
Email: daniel.staegemann@ovgu.de

Klaus Turowski
Very Large Business Applications Lab
Otto von Guericke University
Magdeburg, Germany
Email: klaus.turowski@ovgu.de

Abstract

The goal of this work is to obtain a framework that represents the technological core aspects of blockchain, separated into components, their subcategories and related basic technologies. In order to gain a holistic view of blockchain, with the help of the framework, technologies constructs should be made identifiable as blockchain. For this purpose, a literature review will be conducted to investigate previous approaches to the component-wise division of blockchain technologies. Subsequently, a literature analysis will be conducted in which five established blockchain systems will be analysed and their implementations will be assigned to the general components. For evaluation, a further sixth blockchain technology is used to confirm the basic framework. It becomes apparent that the framework allows a classification of blockchain systems into technologies. The framework has potential for expansion by adding further technology features to make the framework even more useful.

Keywords Blockchain, literature review, technology framework

1 Introduction

Since Bitcoin was introduced by Satoshi Nakamoto in 2008 (Nakamoto 2008), the relevance of blockchain technology has been steadily increasing. In 2018, there were more than 4,600 patent applications in the field of blockchain worldwide in comparison to 43 applications in 2009 (Statista 2019). According to Zhao et al. (2016), the development of the blockchain can be shown in three generations. Starting with Bitcoin as generation 1.0, the blockchain was introduced for the transfer of cryptocurrencies. Since then, other cryptocurrencies have been created, such as Litecoin or Monero, which are mostly offshoots of Bitcoin (Ahamad et al. 2013). In addition to its use as a cryptocurrency, there have been other opportunities to use the technology for securely processing transactions of various types of data without having a trusted third party involved (Casino et al. 2019; Statista 2018). Ethereum represents the blockchain generation 2.0 by allowing Turing complete code to be executed on the basis of a blockchain. Thus, it can be used to map arbitrary programs, whose execution and associated data is stored within the blockchain. These programs for executing transactions are called Smart Contracts (Wood 2019).

The blockchain is continuously being developed to make the advantages of this technology available for more specific industries and applications. Examples of this are the use of blockchain in the healthcare industry (Zhang et al. 2018) or in the field of Internet of Things (IoT) (Andres 2018). In their literature review, Casino et al. have presented an overview of these and other core areas for which blockchain systems are used and referenced further work on them (Casino et al. 2019). These blockchain applications are called Blockchain Generation 3.0 (Zhao et al. 2016).

An important question to ask before introducing a blockchain system is whether there is a specific demand or whether common systems, such as mapping data in a database, are sufficient. In previous research, authors have created frameworks that should provide information about when a blockchain makes sense for a certain use case under certain conditions, and what type of blockchain should be used. For this purpose, several characteristics are highlighted, which a blockchain offers depending on its type. Based on these characteristics and the application case, it can then be decided to what extent a blockchain is a suitable solution. Once, a decision is made in the sense of purpose, the question remains open how it can be implemented and what possibilities exist (Lo et al. 2017; Wüst and Gervais 2018).

This work is intended to take this as a starting point and provide a construction kit that is based on a component-wise consideration of blockchain similar to the existing overviews, but with a greater focus on the technological processes behind these components and the basic technologies used. The goal of the work is to give orientation for blockchain developers by separating the crucial technological aspects and thus demystify the term blockchain. For this purpose, the most important components of the blockchain will be identified in a structured literature review of the existing work. In an enhanced analysis, different blockchain systems will be compared in order to develop a framework that should show the different implementation possibilities of the identified central components, which are used in established blockchain systems.

The main research question is to be answered whether blockchain systems can be represented in a general framework of components in order to identify technology systems as blockchain and to classify used technologies.

Following this introduction, in the second section, a differentiation from previous work is made. Subsequent to the presentation of the used methodology, the analysis setting is explained in the third section. The fourth section contains the results of the literature analysis followed by a proposed framework, which should help to better classify blockchain systems based on the previously presented basic concepts. Finally, a validation of the framework is examined and a short discussion as well as an outlook conclude the achievement.

2 Related Work

There are already many studies or taxonomy frameworks that aim to categorize blockchain technologies by their characteristics. Apart from the classification, one goal is usually to explain what technologies are hidden behind the term blockchain. Tschorsch and Scheuermann (2016), Yaga et al. (2018) and Zheng et al. (2018) describe blockchain in this sense by means of its technical components and go into more detail about how it works. However, with the exception of Zheng et al., no

comparison is made between different blockchain technologies, but rather Bitcoin is used as a reference. Zheng et al. compare different systems only with regard to the consensus methods used.

Wüst and Gervais (2018) refer primarily to the decentralization of the network when they describe blockchain. Further, they create a framework that facilitates a comparison with a conventional database in order to decide whether a blockchain with a certain degree of decentralization or a database would be a more suitable choice in a particular use case. In addition to Wüst and Gervais, other works also subdivide the technology in terms of characteristics. To gain a broader understanding of blockchain, Walsh et al. (2016) divide it into eight different characteristics and present four different blockchain archetypes. These are explained in more detail using four different blockchains, each representing one of these types. The focus is more on decentralization and less on basic technological characteristics. Further on, Glaser (2017) emphasizes a higher level of different characteristics into which he classifies certain functionalities. Dinh et al. (2018), Tasca and Tassone (2018) and Xu et al. (2017) come closest to our approach. They also provide a subdivision of the blockchain technology with regard to the specific application of different blockchains in their individual components. Tasca and Tessone partly go one level deeper into the direction of applied basic technologies, but also put a greater focus on characteristic properties such as scalability or decentralization. In this work, different subdivisions and priorities are set for the analysis. Furthermore, this framework refers purely to technical aspects and not to characteristic ones.

3 Methodology

In order to create a general overview of blockchain technology, characteristics and core components of blockchain are identified by a first systematic literature review in the sense of Okoli (2015). The literature analysis was carried out using a keyword search on the Google Scholar platform. The keywords included the term "Blockchain" in connection with further specifying terms: Technology, Overview, Framework, Security or Network. From the results obtained, German and English language publications not older than ten years were included due to the short history of blockchain. From there, further literature was searched for via references in the papers (Webster and Watson 2002). In terms of content, the works that consider and classify the blockchain technology in its entirety or certain aspects in general were examined more closely. Papers that are specifically aimed at a certain use case were left out.

During the research it became clear that different blockchain systems share basically the same components but realize them differently by using varying approaches. Raikwar et al. (2019) have investigated different blockchains with regard to the used cryptography. As a result of their work, they have created a list of more than 20 different cryptographic concepts that are used in different blockchains. In addition, there are also many different ways to reach agreement on the state of the ledger in the network (Baliga 2017). Furthermore, as examined in Bitcoin, the network itself, its topology, message propagation, or node discovery mechanisms are factors that have different degrees of implementation (Decker and Wattenhofer 2013). Other works, as mentioned in Related Work, look at Blockchain as a whole and break down the technology into individual components. Therein, categories such as architecture, ledger or the block itself are highlighted. In addition, general security, specific hash algorithms and asymmetric cryptography are overarching themes. Further aspects are transactions and their processing, the network and consensus procedures (Tschorsch and Scheuermann 2016; Yaga et al. 2018; Zheng et al. 2018). In general, after analysing these different works, it can be stated that blockchain technologies can be divided into several building blocks, each of which contributes a crucial part to the system.

Seven different components could be iteratively detected, which will be used to further investigate specific implementations of blockchain technologies. In addition, questions about the implementation of each component arise during the research. These questions provide orientation to enable a more specific search and ultimately to set a framework for the analysis. The identified components and the corresponding questions are the following:

Component	Question
Ledger	How do individual blocks get to the Blockchain together?
	What exactly happens in a block saved?
	Which data structures are used for storage of blocks?
	Which hashing algorithm is used?
Roles	What roles can a participant take on in the network?
	Which role has which powers?
	Which role has which data status?
Identification Management	How are users and their property identified?
Network	What is the topology of the network?
	Are there sub-topologies among the participants?
	Are there higher-level protocols?
	On which principle is communication in the network generally based?
	How to find other participants?
	How are connections to other participants established?
	How does a participant receive the current block chain status?
	How are blocks, transactions and messages sent and distributed in the network?
Transactions	Which transaction model is used?
	How are transactions generally executed?
Consensus	Which consensus algorithm is used?
Local storage	How is the block chain stored locally with the participants?

Table 1. Questions related to blockchain component analysis

In order to investigate the specific implementations of blockchains, the literature analysis is enhanced by the examination of five different, established blockchains. The implementation structures and the basic technologies are determined following the pronounced questions. To this end, with reference to scientific literature, special attention will be paid to the resources that the developers of the respective blockchains make available to perform a qualitative analysis of the components. This includes white papers, online documentation, blog and wiki entries. In the course of the analysis, similarities and differences between the technologies are highlighted and recorded. Finally, the results are used to create a framework that depicts the individual components in their variants and provides an overview of the implementation options within them. In the sense of the followed Design Science approach (Hevner et al. 2004), the framework represents an artefact for solving the research question. The construct will show the subdivision of blockchain technologies into basic components. Furthermore, it will be demonstrated how other blockchain systems can be classified with the framework as a first step to evaluate the framework (EVAL 1) according to Sonnenberg and vom Brocke (2012).

According to Coinmarketcap[1], there are more than 1400 different coins in the cryptocurrency market, each of which has its own purpose and can contain different characteristics in its implementations. It would be impractical and would require an enormous effort to include all of them. Therefore, this analysis is limited to five central and widely used blockchain technologies. When selecting the blockchains to be examined, on the one hand the decision is made on the blockchain technologies Bitcoin, Ethereum and Ripple, since these had the largest market share in the cryptocurrency market at the time of the literature research. On the other hand, Hyperledger Fabric is included, because of its relevance for companies and organizations as a private blockchain. Furthermore, the analysis focus on IOTA, which is based on the application of a Directed Acyclic Graph instead of the classical blockchain data structure that represents a different approach compared to others (IOTA Foundation 2020). Simultaneously, this selection includes at least one representative of each of the mentioned blockchain generations (Zhao et al. 2016). Bitcoin and Ripple would be assigned to the first generation, while Ethereum and Hyperledger Fabric would be assigned to the second and IOTA to the third generation. In conclusion, the selection is conducted in a qualitative manner (Yin 2002).

It should be emphasized that not every special feature of the individual technologies will be discussed unless it is relevant to the purpose of the work. This work is intended to provide a holistic overview of

[1] https://coinmarketcap.com

blockchain and its core components. For further information beyond that, the explanations refer to more detailed literature.

4 Blockchain Technology Framework

For the analysis of the particular blockchains, the components to be investigated were determined in advance. For each blockchain, notes were made on the former mentioned questions during the analysis. Due to space restrictions and the mass of information collected, a comprehensive presentation is omitted at this point. The results are summarised and integrated in the component-wise reports in the next paragraphs.

After the single analyses, the cross analysis of the various blockchains shows that similar basic concepts can be found across the board, which are partly identical and partly different in their design. In the following framework, depicted in Table 2, all the technologies explained are arranged according to their respective criteria. Starting from the seven upper criteria, which were identified at the beginning of the analysis, these can be subdivided into further sub-criteria, which in turn can be divided into applied basic technologies that are implemented within the examined blockchains.

Starting with the ledger, Bitcoin, Ripple and Hyperledger Fabric follow the classic blockchain approach, in which one block is lined up after the other and these are connected with a hash pointer (Nakamoto 2008). Ethereum uses its own variant of the GHOST protocol (Sompolinsky and Zohar 2015). This is similar to the classic approach, except that the structure is not a linked list, but a tree-like structure, since blocks are also published and appended (Ethereum Foundation 2020). IOTA follows an approach that goes even further away from the original idea and uses a directed acyclic graph (DAG) that connects individual transactions (IOTA Foundation 2020). For chaining, all technologies use hash pointers, but with different hash algorithms. Bitcoin relies on SHA-256, Ripple on halved SHA-512. Hyperledger uses SHA3 SHAKE 256 (Nguyen 2016), Ethereum Keccak-256 (Wood 2019) and IOTA the curl algorithm. Another sub-criterion of the ledger is the memory structure used within a block to store transaction data and possibly account data. Bitcoin and Ripple use the Merkle Tree for this purpose, while Ethereum and Hyperledger use modifications in the form of Merkle-Patricia Tree and Bucket Hash Tree (Xu et al. 2017).

The second upper criterion shows the roles that can be adopted within a system. The type of role depends on whether a user participates in the network as a full or thin client. Inventory servers exist in all systems and represent the classic participants and the majority of all nodes. In addition, all systems have a form of validator that participates in the consensus process and ensures that transactions are validated and published for an equally distributed ledger. In Bitcoin and Ethereum, these are miners who, due to the consensus mechanism, receive a reward in the form of the internal cryptocurrency. Ripple, IOTA and Hyperledger are partially centralized systems. In Ripple there is only a certain number of validators known in the network. In the other two, central roles in the form of the coordinator or ordering node ensure publication. In Ethereum, Ripple and IOTA, the participants do not necessarily have a copy of the ledger with all data up to the Genesis block. For this reason, archive nodes or permanent nodes are used there that store the full history so that it can be made available to others as required. Ethereum and Hyperledger use Smart Contracts. In Ethereum they hold an own account while in Hyperledger, they are held by endorsing peers who make their functionality available to other nodes. In Ripple and Hyperledger there are additional roles to enable their network structure. Since other currencies can be traded in Ripple, some participants in the network (e.g. banks) act as gateways and offer different currencies. In Hyperledger, the network consists of several channels that are isolated from each other. In order to communicate between these channels, there are anchor peers that can connect to nodes of a foreign channel to exchange information. Each channel also contains a Leader Peer, which is the recipient of newly validated transactions published by the Ordering Node. The Leader Peer is then responsible for forwarding these to everyone else in the channel (Bitcoin Project 2020; EthHub 2020; Hyperledger 2020; IOTA Foundation 2020; XRP Ledger Project 2019).

The next critical component is the implementation of a user identification. In open blockchains (e.g. Bitcoin, Ethereum), user anonymity must be guaranteed, while transactions and account data must be clearly assigned to them. All discussed blockchains use asymmetric cryptography. Public keys are used as user addresses, which are first hashed and then encoded for display. The hashing algorithms used are the same as those used for the hash pointers with the exception of IOTA, which uses the Kerl algorithm and Winternitz scheme for one-time signatures. For encoding, Bitcoin and Ripple use the Base58 Encoding Scheme. Ethereum uses mixed-case checksum address encoding (Ethereum Foundation 2020) and IOTA uses tryte encoding (IOTA Foundation 2020). The private key is used to create digital signatures. Bitcoin, Ethereum and Ripple use the elliptic curve ECDSA while Ripple

refers to the EdDSA curve. Hyperledger implements a user register for administration tasks. All network users receive an X.509 certificate that contains their data and keys, by which they are identified (Hyperledger 2020).

Without exception, a peer-to-peer network is implemented in all blockchain technologies. Except for Hyperledger Fabric, the topologies are random or a mesh network in which peers can have multiple outgoing and incoming connections to other peers (Decker and Wattenhofer 2013). In Hyperledger, the validating peers form a subsidiary mesh network. Further, Hyperledger Fabric is a multichain network in which each network can serve a different purpose. In the other blockchains, additional sub-topologies exist within the network. In Bitcoin, miners can join together to form mining pools (Miller et al. 2015). In Ripple, validators maintain a Unique Nodes List that includes other peers with whom connections are made to coordinate on consensus. Ripple also offers the possibility to create a private network where only selected peers can connect (XRP Ledger Project 2019). REST (Bitcoin, Ripple and Hyperledger Fabric) and JSON RPC API interfaces (Ethereum and IOTA) are implemented for messaging through the network. Communication within the network between the nodes takes place via protocols that basically follow a request-response scheme. When a peer wants to establish a new connection with another peer or requests missing transactions or blocks, a request is first made, after which the other peer responds with the requested information. Each technology uses its own communication protocol. Bitcoin uses its Network P2P protocol (Bitcoin Project 2020), Ripple the RTXP Peer Protocol (XRP Ledger Project 2019) and Hyperledger Fabric the Gossip Data Dissemination Protocol (Hyperledger 2020). Ethereum uses different protocols and separates between the Node Discovery protocol and the RLPx protocol for further communication, which has other subprotocols that peers agree on when connecting to each other (Antonopoulos and Wood 2018). For peer discovery, various methods are used within the networks. All networks use trusted hard-coded nodes for initial connections via boot nodes, DNS seeds or public hubs. In addition, further nodes can be found in the network via various methods. For this purpose, requests can be sent to connected nodes via the Gossip Protocol, which send back data about parts of their neighbors. Similarly, Ethereum uses Recursive Look-Ups to find node. In IOTA, manual peering is currently used for discovery and connection with other nodes, but this is to be replaced by automatic peering in the future (IOTA Foundation 2020). The connection to other nodes is pseudo-random in Bitcoin, Ethereum and IOTA. Requests for connection are sent to the peers during discovery. Ethereum and IOTA additionally use distance measurement, that calculate distances to the other peers from the public keys and select with whom a connection is made. In Ripple it is possible to enter into connections with fixed, previously determined peers and to reserve free spaces for them. Since Hyperledger Fabric has a private network, connections are predetermined, as only nodes from the same or different organizations connect to form a common consortium and pursue a common goal (Hyperledger 2020). Gossip protocols are used to propagate new transactions on the network. These ensure that transactions are sent to all connected peers, who in turn forward them.

Furthermore, the processing and execution of transactions forms an upper criterion in all blockchain systems. A general distinction must be made between the UTXO model used by Bitcoin (Bitcoin Project 2020; Nakamoto 2008) and the account-based model introduced by Ethereum (Antonopoulos and Wood 2018) that is likewise integrated in the other examined blockchains, whereby Hyperledger leaves open which model is used in order to be able to serve all use cases. A differentiation exists further in transaction execution. Bitcoin provides only a limited number of commands, which are available via their scripting language. The situation is similar within Ripple and IOTA, which are planning to introduce smart contracts that already used by Ethereum and Hyperledger Fabric (Hyperledger 2020; IOTA Foundation 2020; XRP Ledger Project 2019)

The penultimate upper criterion of the framework deals with the consensus procedures. Bitcoin and Ethereum as open blockchains rely on the proof of work, that implement a hash puzzle with the SHA-256 hash function and the Ethash. Hyperledger Fabric and Ripple have a centralized approach to consensus with the Byzantine Fault Tolerance Protocol. In IOTA a Tip Selection in combination with the Coordinator is currently in use as a central network component. The Coordinator shall be replaced by a voting mechanism in the form of a Fast Probabilistic or a Cellular Consensus (Ethereum Foundation 2020; Hyperledger 2020; IOTA Foundation 2020; Nakamoto 2008; XRP Ledger Project 2019).

Ultimately, differences can be seen in the local storage of ledger data. Increasingly, databases in the form of key-value stores are being used and save meta data that refers to files that store the block data. In all applications except IOTA, LevelDB is used for this purpose. Bitcoin and Ethereum also use RocksDB (Bitcoin Project 2020; Wood 2019) and Ripple NuDB (XRP Ledger Project 2019). Hyperledger Fabric is compatible with CouchDB in addition to LevelDB (Hyperledger 2020). While in

all technologies the block data is stored in flat files, IOTA stores the tangle using snapshots of it (IOTA Foundation 2020).

Upper Criterion	Sub-criterion	Basic Technology	Specification
Ledger	General data structure		Blockchain, GHOST, Directed Acyclic Graph
	Linkage	Hash pointer	SHA-256, SHA-512 Half, Keccak-256, SHA3 SHAKE256, Curl
	Storage of transactional data	Data structures	Merkle tree, Merkle Patricia tree, Bucket hash tree
Roles	Client	Full Client	
		Thin Client	
	Node	Inventory Server	
		Miner / Validator	
		Gateway	
		Archive Node / Permanode	
		Orderer Node / Coordinator	
		Leader Peer	
		Anchor Peer	
		Endorsing Peer / Smart Contract	
Identification Management	Transaction Identification	Digital Signatures	ECDSA with secp2kl, EdDSA with Ed25519, Winternitz (One Time Signature Scheme)
	Users / Ownership	Hash-Address	SHA-256, RIPEMD160, SHA-512 Half, Keccac 256, Kerl
		Encoding	Base58, Mixed-case Checksum Encoding, Tryte Encoding
	Membership	Certificate	X.509
Network	Type	Peer-To-Peer-Network	
	Topology	Random	
		Mesh	
		Chain	
	Sub-Topology	Mining Pools	
		Privat Network	
		Unique Node List	
		Channels	
	Protocols	Message protocol	Network P2P Protocol, Node Discovery Protocol, RLPx Protocol, RTXP Peer Protocol, Gossip Data Dissemination Protocol
		Transaction protocol	Gossip Protocol
	Communication	Client-Node-Connection	REST API, JSON RPC API
		Messaging Pattern	Request-Response-Pattern
		Peer Discovery	Public Hubs / Bootnodes, DNS Seeds, Request Peers via Neighbours, Recursive Look-up
		Peer Connection	Random, Fixed/Reserved Peers, Manual Peering, Auto Peering
Transactions	Transaction model	Account-based	
		Transaction-based	UTXO model
	Transaction execution	User-based	
		Code-based (Turing complete)	Solidity
		Code-based (unspecific)	OPCodes
Consensus		Proof-of-work	Hash puzzle
		Byzamtine Fault Tolerance	
		Tip-Selection + Coordinator	
		Tip-Selection + Voting Mechanism	
Local storage	Database	Key-Value-Store	RocksDB, LevelDB, NuDB, CouchDB
		File-based	Flat-files, Snapshots

Table 2. Blockchain Technology Framework

5 Evaluation

The evaluation is intended to justify the theory in the form of the framework by using another blockchain to answer the initial questions of this research work. It will show that this blockchain can be inserted into the framework and thus identify it as a blockchain system. Further, the components can be applied in the previously identified upper and lower criteria, thus confirming the framework we have set for the classification of blockchain technologies.

The blockchain "Symbol" from NEM is chosen for validation, whose white paper was published at the beginning of 2020. Symbol is a development platform for public, private or hybrid blockchains.

Symbol blockchains work according to the philosophy originally introduced by Bitcoin, where each participant holds a copy of the blockchain and can verify it. In addition, anyone with sufficient harvesting power can create new blocks and does not need to rely on a central instance (NEM 2020).

The ledger as the first component is identified. As in the other technologies, with the exception of IOTA, a block is made up of a header and a body. The body contains a list of transactions and the header contains information that describes the block in the overall context of the blockchain. Blocks are connected to each other by a SHA3-256 hash pointer and, in addition to the transactions, store a reference hash to receipts, transaction documents and the blockchain state. The transaction and receive hash is stored in a Merkle tree while the state hash in a Patricia tree.

Participants in the network can assume two roles. On the one hand there are peers who can create new blocks and participate in the harvesting process. Harvesting is equivalent to mining in Bitcoin when using NEM. They verify transactions and blocks, propagate changes in the network, connect and synchronize with other peers. On the other hand, there are API nodes that store blockchain data in a MongoDB for easier searching and can be used by a client application in combination with a NodeJS REST server. API-Nodes synchronize themselves with others, but do not participate in the harvesting process. It is also possible to act as a dual node and combine the characteristics of both roles.

Each participant is assigned to an account for identification purposes. The address of this account is generated from the public key of a cryptographic key pair and encoded in Base32. During this process the 256-bit SHA3 and the 160-bit RIPEMD hash function is used. Digital signatures are used to sign transactions as in the other blockchains. Symbol uses these in the form of the Ed25519 Elliptic Curve.

The NEM network is a P2P network in which a request-response protocol is used to establish connections, general communication between nodes, and transactions distribution. To ensure that the ledger statuses of all nodes are the same, they are periodically synchronized with each other. A node asks one of its partners for the ledger status of the other node. If the blockchain is valid and up-to-date, the blockchain is adopted. A discovery protocol is used to discover new nodes. First, a new node makes random connections with a random subset of beacon nodes. These are nodes recorded in a config file, which serve a first step into the network. Nodes periodically send information about themselves to all nodes they know, in order to be added to their list of potential partners for synchronization. Furthermore, periodic requests are sent to all known nodes to get all information about their known nodes in order to be able to connect to them directly. In general, existing connections are periodically terminated and then new ones are established to prevent nodes from connecting in a targeted manner. With whom a connection is finally made depends on the reputation of possible partners. This is based on a score, which is formed from the number of transactions made and the success rate. The more transactions and the higher the success rate, the higher the probability that a connection will be made with this node, as it has a high reputation. Another concept is node banning. NEM has established rules to banish nodes and restrict connections for a certain period of time in the future. A node will be banned if another node receives invalid data from it.

Symbol uses an account-based transaction model in which account data is stored in the blockchain state. As in the other blockchain systems, transactions are the only way to change the state of the blockchain in any way.

Regarding the transactions, Symbol differs between two types, the transfer transaction and the aggregated transaction. The former sends Mosaics from one account to another, while the latter merges several transactions. Mosaics are fixed assets that cannot been changed. They can be tokens, for example, but also a collection of more specific values such as reward points, stock shares, votes or other currencies. Smart Contracts are not implemented for transaction execution but a plug-in architecture. Although, it limits the possibilities, it reduces the attack surface. Otherwise, it gives more flexibility than the defined transaction types as in Bitcoin.

All participants in the network must support the same set of transaction plug-ins and execute them in the same way thus the ledger is always identical among them. All transactions in Symbol are created by using the plug-in model. A selection from standard plug-ins that meet network requirements of a developing blockchain can be made while one can additionally implement own plug-ins to extend the Symbol protocol. Besides plug-ins there are also extensions that has not to be used by all nodes, as they do not influence the consensus process. These extensions allow nodes to integrate individual capabilities. For example, you can create dependent services or subscribe to certain blockchain events to be notified when state changes occur.

To achieve consensus, the proof-of-stake is used, but in a modified form that incorporates core elements of the proof-of-importance. With proof-of-stake, unlike proof-of-work, the likelihood of

success does not depend on the hash rate, but on the prosperity of the user. This means that the more shares a user has in the network, the more incentives he has to keep the network alive and therefore has a higher chance to harvest a new block. The problem here tends to be that rich users become richer and poor stay poor. In order to smooth the chances, concepts of proof-of-importance are now being added, hence, active users, rather than hoarders, benefit. Thus, two more factors are integrated in the determination of the importance of a user for the network. At first, the number of executed transactions of a user are included that can be expressed in terms of fees that an account has paid. The second factor refers to the number of nodes a user controls that is measured by how many times a user has been the beneficiary of a block publication. Since a user who controls a node itself defines which account will receive the reward for creating a new block. The importance score is periodically recalculated from the three factors and thus provides a weighted random choice of who may create the next block.

In Symbol, nodes store all data in flat files as data directories. Peer nodes store the state in RocksDB files wherein cached data is serialized and stored as key-values. Further, API nodes hold blocks, transactions and states in MongoDB for fast access. The data is loaded into a directory called "spool", which forms a file-based queue. A broker service takes the data from the spool, updates MongoDB accordingly and notifies REST instances of changes if they have subscribed to it.

After analysis of the Symbol blockchain of NEM, the selection of the framework's upper criteria can be confirmed. These could be easily identified and assigned. However, considering the deeper levels of the framework, it is noticeable that Symbol has aspects that have not yet been implemented by other blockchains. In the network, the reputation system can be used to add a new way of selecting connection partners. In addition, the node banning could be used to add another sub-criterion for the network. When executing transactions, Symbol does not rely on a strict specification of transaction types to be processed or on the use of Smart Contracts. In the case of consensus algorithms, there are two approaches, proof-of-stake and proof-of-importance, which have not been used before. Furthermore, MongoDB is an application that has not been observed before for the storage of block data. Thus, the initial questions, which are to be answered with this framework, can only be answered partially. Symbol can be identified as a blockchain with the help of the framework, since all upper criteria recur and all of the sub-criteria are applied. The basic technologies used are largely the same, while new ways of implementation have been established. Thus, the question of which components one should generally pay attention to when developing a blockchain can be answered. In contrast, the question of a holistic overview of previous implementation strategies and the basic technologies used for the individual components cannot yet be answered completely.

Overall, it can be concluded that the framework in this form presents an appropriate structure of blockchain systems. The choice of the upper criteria could be confirmed. Possible additions could already be identified for the sub-criteria as well as for the basic technologies used. As already mentioned, there are over 1000 different blockchain technologies, which cannot all be represented by this framework in the current state. Finally, further research has to extend the technology framework by more specifications of basic technologies.

6 Discussion and Conclusion

As things stand, the framework gives an overview of what a blockchain means to be and which technical components can be used to identify it. In addition, it includes important functionalities in a blockchain and to which components and specific basic technologies they are assigned. Multiple literature reviews were conducted to design the framework in the sense of Design Science (Hevner et al. 2004). Regarding the research question, the analysis of several blockchain technologies shows that a blockchain could be classified by the proposed frame. In addition, the integration of another blockchain system demonstrates the identification of a blockchain technology and presents a first step of evaluation (Sonnenberg and vom Brocke 2012).

Tasca and Tassone (2018) took a similar approach of a framework and investigated several blockchains according to different categories. Compared to this work, less focus was placed on blockchains as a composition of technological components, but more on blockchains and their general characteristics. An important factor is who can participate within the blockchain and what rights each participant has. This characteristic is represented by an established categorization of public, federated and private blockchains. It is decisive whether read and write rights as well as block validation is accessible to everyone or only previously authorized nodes have permission for certain activities. Depending on the use case, the design of the consensus process has different requirements. The propagated Blockchain Technology Framework (BTF) take that into account by the upper criterions of Identification

Management and Consensus. A suitable selection of basic technologies ensures the implementation of different types of blockchain regarding permissions and public participation.

Another factor is the direct integration of Smart Contracts and cryptocurrencies into the framework of Tasca and Tassone (2018). While a Smart Contract can be represented either by a specific node, transaction code or an external plug-in, a simple criterion as a characterisation would not be sufficient. Therefore, Smart Contracts are not directly presented in the BTF because it depends on their implementation. Likewise, cryptocurrencies could be realised as UTXO tokens or as transactions booked in the ledger.

Other characteristics like scalability and throughput are related to the technical realisation of the P2P network, the topologies and the network nodes. An assessment of these base technologies allows a determination of the qualities of a blockchain system.

In conclusion, a framework, beyond the identification and assignment of the blockchain, its components and base technologies, could provide a precise answer to how the design of a blockchain with specific requirements for the individual components and characteristics could look like. For this purpose, a feature tree from a software engineering perspective could be developed with the help of the framework that shows the composition of the individual components in relation to the various requirements for the characteristics. In order to realize that, more blockchain systems would have to be investigated in future work to complete the range of technologies that can be chosen from. The implementation of a case study analysis according to Eisenhardt (1989) would be conceivable. In addition, a decision on the necessity of blockchain technology in application use cases could be made by an appropriate requirements engineering.

7 References

Ahamad, S., Nair, M., and Varghese, B. 2013. "A Survey on Crypto Currencies," *4th International Conference on Advances in Computer Science* (2013), pp. 42–48.

Andres, C. 2018. *Entwurf Und Prototypische Implementierung Eines Blockchain-Basierten IoT-Software-Update-Systems*, Abschlussbericht FEP 2018, Fachhochschule Münster.

Antonopoulos, A. M., and Wood, G. 2018. *Mastering Ethereum*, O'Reilly Media. (https://github.com/ethereumbook/ethereumbook).

Baliga, A. 2017. "Understanding Blockchain Consensus Models." (https://www.semanticscholar.org/paper/Understanding-Blockchain-Consensus-Models-Baliga/).

Bitcoin Project. 2020. "Developer Guides." (https://developer.bitcoin.org/devguide/index.html).

Casino, F., Dasaklis, T. K., and Patsakis, C. 2019. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," *Telematics and Informatics* (36), pp. 55–81. (https://doi.org/10/ggjjph).

Decker, C., and Wattenhofer, R. 2013. "Information Propagation in the Bitcoin Network," *IEEE P2P 2013 Proceedings*, pp. 1–10.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J. 2018. "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering* (30:7), pp. 1366–1385. (https://doi.org/10/gdqn86).

Eisenhardt, K. M. 1989. "Building Theories from Case Study Research," *Academy of Management Review* (14:4), pp. 532–550.

Ethereum Foundation. 2020. "Wiki." (https://eth.wiki).

EthHub. 2020. "Running an Ethereum Node." (https://docs.ethhub.io/using-ethereum/running-an-ethereum-node/).

Glaser, F. 2017. "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*, AIS, pp. 1543–1552. (https://doi.org/10/gfwwnv).

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75–105.

Hyperledger. 2020. *A Blockchain Platform for the Enterprise*. (https://hyperledger-fabric.readthedocs.io/en/release-2.0/).

IOTA Foundation. 2020. "Developer Documentation." (https://docs.iota.org/).

Lo, S. K., Xu, X., Chiam, Y. K., and Lu, Q. 2017. "Evaluating Suitability of Applying Blockchain," in *IEEE 22nd International Conference on Engineering of Complex Computer Systems*, Fukuoka, Japan, pp. 158–161.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." (https://bitcoin.org/bitcoin.pdf).

NEM. 2020. "NEM Symbol: Technical Reference." (https://docs.symbolplatform.com/catapult-whitepaper/main.pdf).

Nguyen, B. 2016. *Protocol Specification*. (https://github.com/hyperledger-archives/fabric/blob/master/docs/protocol-spec.md).

Okoli, C. 2015. "A Guide to Conducting a Standalone Systematic Literature Review," *Communications of the Association for Information Systems* (37), pp. 879–910. (https://doi.org/10/ggnjdd).

Raikwar, M., Gligoroski, D., and Kralevska, K. 2019. "SoK of Used Cryptography in Blockchain," *IEEE Access* (7:1), pp. 148550–148575. (https://doi.org/10.1109/ACCESS.2019.2946983).

Sompolinsky, Y., and Zohar, A. 2015. "Secure High-Rate Transaction Processing in Bitcoin," *International Conference on Financial Cryptography and Data Security*, pp. 507–527. (https://doi.org/10/gfwwk7).

Sonnenberg, C., and vom Brocke, J. 2012. "Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research," in *Design Science Research in Information Systems. Advances in Theory and Practice* (Vol. 7286), Lecture Notes in Computer Science, K. Peffers, M. Rothenberger, and B. Kuechler (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 381–397. (https://doi.org/10.1007/978-3-642-29863-9_28).

Statista. 2018. "Verteilung Der Blockchain-Startups in Deutschland Nach Kategorien (Stand: April 2018)." (https://de.statista.com/statistik/daten/studie/871944/umfrage/blockchain-startups-in-deutschland-nach-kategorien/).

Statista. 2019. "Anzahl Der Weltweiten Blockchain-Patentanmeldungen pro Jahr von 2008 Bis 2019." (https://de.statista.com/statistik/daten/studie/1062733/umfrage/anzahl-der-weltweiten-blockchain-patentanmeldungen-pro-jahr/).

Tasca, P., and Tessone, C. J. 2018. "Taxonomy of Blockchain Technologies. Principles of Identification and Classification." (http://dx.doi.org/10.2139/ssrn.2977811).

Tschorsch, F., and Scheuermann, B. 2016. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys & Tutorials* (18:3), pp. 2084–2123. (https://doi.org/10/gfwwnm).

Walsh, C., O'Reilly, P., Gleasure, R., Feller, J., Li, S., and Cristoforo, J. 2016. "New Kid on the Block: A Strategic Archetypes Approach to Understanding the Blockchain," in *Thirty Seventh International Conference on Information Systems*, Dublin, Ireland: AIS.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii–xxiii.

Wood, G. 2019. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. (https://ethereum.github.io/yellowpaper/paper.pdf).

Wüst, K., and Gervais, A. 2018. "Do You Need a Blockchain?," in *Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, pp. 45–54.

XRP Ledger Project. 2019. *XRP Ledger Documentation*. (https://xrpl.org/docs.html).

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. 2017. "A Taxonomy of Blockchain-Based Systems for Architecture Design," in *IEEE International Conference on Software Architecture*, Gothenburg, Sweden, pp. 243–252. (https://doi.org/10.1109/ICSA.2017.33).

Yaga, D., Mell, P., Roby, N., and Scarfone, K. 2018. *Blockchain Technology Overview*, Gaithersburg, MD: National Institute of Standards and Technology.

Yin, R. K. 2002. *Case Study Research - Design and Methods*, (3rd ed.), Applied Social Research Methods Series, Thousand Oaks, CA: SAGE Publications.

Zhang, P., Schmidt, D. C., White, J., and Lenz, G. 2018. "Blockchain Technology Use Cases in Healthcare," in *Blockchain Technology: Platforms, Tools and Use Cases* (Vol. 111), Advances in Computers, Elsevier, pp. 1–41.

Zhao, J. L., Fan, S., and Yan, J. 2016. "Overview of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue," *Financial Innovation* (2:1). (https://doi.org/10/gfkn4d).

Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. 2018. "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services* (14:4), pp. 352–375.