Research Center
Finance & Information Management

Fraunhofer FIT
Project Group
Business & Information
Systems Engineering

Discussion Paper

BLOCKCHAIN AND SMART CONTRACTS
Technologies, research issues and applications

by

Julian Schütte[1], Gilbert Fridgen, Wolfgang Prinz[2], Thomas Rose[2], Nils Urbach, Thomas Hoeren[2], Nikolas Guggenberger[3], Christian Welzel[4], Steffen Holly[5], Axel Schulte[6], Philipp Sprenger[6], Christian Schwede[6], Birgit Weimert[7], Boris Otto[8], Mathias Dalheimer[9], Markus Wenzel[10], Michael Kreutzer[11], Michael Fritz[12], Ulrich Leiner[12], Alexander Nouak[13]

April 2018

[1] Fraunhofer AISEC
[2] Fraunhofer FIT
[3] Universität Münster
[4] Fraunhofer FOKUS
[5] Fraunhofer IDMT
[6] Fraunhofer IML
[7] Fraunhofer INT
[8] Fraunhofer ISST
[9] Fraunhofer ITWM
[10] Fraunhofer MEVIS
[11] Fraunhofer SIT
[12] Zentrale der Fraunhofer-Gesellschaft
[13] Fraunhofer-Verbund IUK-Technologie

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: Wittelsbacherring 10, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-780

Fraunhofer

BLOCKCHAIN AND SMART CONTRACTS

Technologies, research issues and applications

BLOCKCHAIN AND SMART CONTRACTS

Technologies, research issues and applications

Editors:

Wolfgang Prinz
Fraunhofer Institute for Applied Information Technology FIT

Axel T. Schulte
Fraunhofer Institute for Material Flow and Logistics IML

Authors:

Julian Schütte, Fraunhofer AISEC
Gilbert Fridgen, Fraunhofer FIT
Wolfgang Prinz, Fraunhofer FIT
Thomas Rose, Fraunhofer FIT
Nils Urbach, Fraunhofer FIT
Thomas Hoeren, Fraunhofer FIT
Nikolas Guggenberger, University of Münster
Christian Welzel, Fraunhofer FOKUS
Steffen Holly, Fraunhofer IDMT
Axel Schulte, Fraunhofer IML
Philipp Sprenger, Fraunhofer IML
Christian Schwede, Fraunhofer IML
Birgit Weimert, Fraunhofer INT
Boris Otto, Fraunhofer ISST
Mathias Dalheimer, Fraunhofer ITWM
Markus Wenzel, Fraunhofer MEVIS
Michael Kreutzer, Fraunhofer SIT
Michael Fritz, Headquarters of the Fraunhofer-Gesellschaft
Ulrich Leiner, Headquarters of the Fraunhofer-Gesellschaft
Alexander Nouak, Fraunhofer ICT Group

Published in April 2018

Blockchain | en | 1st print | v1.6—apr18 | hko | 200pcs.

CONTENT

SUMMARY

This position paper analyzes blockchain technology from the scientific and application-oriented perspective of the Fraunhofer-Gesellschaft. It examines relevant technical aspects and related research questions. It shows that technology still has fundamental research and development challenges in all areas. These include, for example, the modularization of individual blockchain concepts as well as their combination and integration for application-specific blockchain solutions.

Fig. 1: Technology, applications and competencies from the point of view of the Fraunhofer-Gesellschaft

The investigation of fields of application and industries which are most likely to benefit from the new technology shows that different properties of blockchain are relevant to each field of application. While the automation potential associated with smart contracts is particularly essential for the Internet of Things, the irreversibility of managed transactions is of major importance for applications in the areas of supply chain, digital media, and proofs of origin. What is crucial, however, is the aspect that the blockchain has a high degree of relevance for many different application areas which are outside of the financial industry and, above all, independent of crypto currencies. The paper provides a list of criteria for identifying applications that are suitable for using a blockchain.

The business and politics fields are currently dealing intensively with the challenges and potential of digitization. Developments in the context of blockchain technology, as shown in this paper, will have a major impact on the design and implementation of digital business processes as well as e-government solutions and, therefore, also on social processes. Diverse initiatives and consortia are beginning to set international standards that require early interagency participation, since issues relating to law, tax, research policy and economics are raised in this process. At the political level, a comprehensive regulatory framework needs to be created that enables innovation while also considering civic rights. This requires to examine the relevant legal certainty, which should aim at testing the legal validity of the declarations stored in a blockchain, taking into account their functional and cryptographic characteristics. In addition, since blockchain applications are not limited to a national level, investigations and piloting of the legal consequences of transnational blockchains should also be started, at least at the EU level as well as beyond.

For blockchain-based solutions to be able to establish extensive new business models, it is necessary to examine the use of blockchains even in highly regulated sectors (energy, finance, medicine, public processes). If needed and after a positive evaluation of pilot implementations, the use of the technology should be made possible through appropriate legislative changes.

On a research policy level, the paper recommends activities that focus, above all, on aspects of standardization and certification of smart contracts. It is expected that patterns and templates will emerge for frequently used applications, as well as marketplaces for smart contracts in the next step. In order to develop reliable standard building blocks, it is necessary to establish testing bodies and certification bodies, as well as libraries and marketplaces, through which smart contracts are offered and, above all, provided to SMEs. This also has to include warning systems for handling detected vulnerabilities.

In addition to the open and widely distributed blockchains, numerous private, access-controlled blockchain applications are already being developed today. It is expected that there will be a proliferation of blockchain infrastructures with overlapping application contexts. Therefore, it is necessary to set up a blockchain registry to register and announce blockchain infrastructures in various application areas. In the long run, this can create an ecosystem that, for example, enables the interoperable use of blockchain infrastructures for financial transactions, goods tracking and the quality assurance of production data. In concrete terms, the early promotion of such an infrastructure can be implemented with a blockchain for the research landscape in Germany (e-science).

An implementation focused on SMEs is important in the pursuit of these recommendations. This is mainly due to the fact that, on the one hand, SMEs often work together in value creation networks, exactly where blockchain can fully develop its potential. For this reason, appropriate advisory measures for SMEs have to be initiated to develop expertise and education through testing and pilot implementations.

The proposed measures require a multidisciplinary approach, both in the development of basic technologies as well as in application development, profitability analysis and the design of new governance models. The multifaceted competencies of the Fraunhofer institutes enable the Fraunhofer-Gesellschaft to make a significant contribution to the solution of identified research questions and, therefore, to the further development and application of blockchain technology. In order to strengthen the national competitive situation, state support programs should be set up according to the measures proposed here.

1
INTRODUCTION

1.1
Motivation

Since Satoshi Nakamoto published his white paper [16] in 2008 and the first bitcoins were created in early 2009, both cryptocurrencies as well as the underlying technology of the blockchain have received a tremendous amount of attention. The development of blockchain applications is often divided into three phases: Blockchain 1.0 covers the cryptocurrencies, Blockchain 2.0 essentially concerns smart contracts in the financial sector and, in Blockchain 3.0, smart contracts are developed into decentralized autonomous organizational units, with their own laws and a high degree of autonomy, with that applying in nearly all areas. Accordingly, numerous new fields of application and implementation possibilities for blockchain technology, which go far beyond a virtual currency, are currently being developed at a rapid pace.

The basis for this interest is composed by the following characteristics and various potential of the blockchain concept:

- In business processes, the technique of **distributed consensus building** can replace the role of a trusted third party in the areas of process execution and authentication. This concerns intermediaries in the economic context as well as supervisory functions in sovereign duties. It therefore calls into question the business models of many organizations and institutions that now play this role. However, there are also new business models that would not be feasible considering economic matters without blockchain technology. Confidence in a third party is being replaced by trust in a collective, trust in a technology and trust in cryptography.

- In blockchain, **values** can be mapped regarding which access rights can be clearly and permanently transferred from one user to another. Therefore, blockchain is seen as the basis of the **Internet of value** and as a supplement to the previous Internet of information. Cryptocurrencies are only the most obvious application. Even rights to **real world values** can be mapped digitally in blockchain and traded as such. This extends the Internet from a platform for copying and sharing into a platform that logs the origins and possession of assets and makes them transparent.

- Even if this does not involve contracts in the legal sense, the concept of **smart contracts** allows for rules and execution instructions to perform predetermined processes on blockchain in an automated and decentralized manner. This opens up enormous **potential for automation**. The range of applications extends from logistics and commerce to the Internet of Things (IoT), with which, for example, intelligent objects can independently negotiate and establish their use.

- Basically, the transactions represented in a blockchain are visible to all participants in the network and are therefore **transparent**. In addition, blockchain promises **irreversibility**, i.e., transactions in blockchain cannot be subsequently manipulated or even deleted. In order to reverse a transaction, it is only possible – again, by consensus – to deposit the corresponding counter transaction in the blockchain. In principle, this will make proofs of origin and transactions safe for mapped values in terms of auditing. This opens up a wide range of possibilities in the field of compliance up to the automated testing of processes that have so far been performed manually, thereby questioning the business models of auditors. If complete transparency is not desired, there is, on the one hand, the possibility of private blockchains to which only a limited number of users have access. On the other hand, there are meanwhile ways and means to limit traceability even in public blockchains – with all the advantages and disadvantages, such as in the darknet (see Section 3.10).

In recent years, these characteristics have led to an explosive development of new applications as well as to an overwhelming number of actors. These range from various start-ups and technology companies to newly formed consortia, such as the *Hyperledger Project*. However, individuals, governments, NGOs, universities, research organizations, and venture capitalists are also researching and developing the next "killer app" which will be for blockchain what the browser was to the Internet [17].

This hype cannot hide the fact that there are currently a lot more visions, theories, and concepts than actually existing examples that really work. This is because the still young and, at the same time, complex technology brings multifaceted challenges in the area of the fundamentals of information and communication technology (ICT) as well as in the field of applications and attack scenarios. The technology currently lacks infrastructures for the respective deployment, adequate capacities, scalability and short reaction times, a coherent governance model and the corresponding legal framework.

Against this background, a core challenge for science and, therefore, also for the Fraunhofer-Gesellschaft, is the critically analytical evaluation of this technology. The question of whether it is a hype or whether the technology has enough disruptive potential depends on many factors that need to be investigated systematically. In this regard, questions that have to be considered include: What opportunities and risks (and for whom) are associated with the technology? What are the obstacles and drivers of the implementation? What effects will the technology have on the economy and public administration, and how can companies and public authorities – whatever the uncertainty – most effectively prepare today? In addition to the identification of technical research questions, this includes the identification of the industries in which the first or the largest changes are expected.

At this interface of technology and application, the scientific knowledge of the Fraunhofer-Gesellschaft is in particular demand. Across the institutes, there is a unique wealth of experience from the development to the comprehensive assessment of new technologies – from technical details to economic evaluation. As a result, the Fraunhofer-Gesellschaft offers itself as a point of contact for the industry when it comes to developing sufficient expertise early on in order to more effectively assess blockchain technology in its own respective environment as well as to make informed decisions about future investments and political framework conditions.

The present position paper of the Fraunhofer-Gesellschaft presents a systematic classification – based on the main fundamentals and characteristics – into the research landscape, as well as a collective representation of the already existing and the conceivable future application possibilities of blockchain technology. The paper also demonstrates the contribution that the Fraunhofer-Gesellschaft can make, based on its expertise, to the further development and implementation of the technology.

1.2
Blockchain fundamentals

The blockchain's ability to irreversibly store transactions and to delegate the sovereignty of a certifying authority to distributed consensus building is based on the combination of different techniques which are presented in simplified form in the following sequence [19].

First, the transaction, such as the transfer of a cryptocurrency or the registration of a document, is generated by a sender and digitally signed. This transaction is sent to the network and distributed to the nodes involved. The nodes of the network check the validity of the transaction and insert it into the blockchain.

In this process, the transactions are stored in blocks which are converted in a standardized format by means of a hash function. First, all individual statements are coded in hash values and then compressed hierarchically. This hierarchical compression of the individual statements is referred to as a hash tree or Merkle tree, by means of which a block of statements can be clearly represented. The coding of the statements is safe against manipulation attempts, since changing one single statement would change the hash value of the block, and the hash tree would therefore no longer be consistent.

Blocks are connected by means of chaining with the already existing history of the blocks, resulting in a chain (blockchain) being created. In order to include a block in the existing chain as a new element, in the bitcoin use case a cryptographic puzzle has to be solved: which string provides a similar hash value as the encoding of the new block that is to be implemented. The similarity of both values is defined by the number of characters to be matched in the hash value. The degree of complexity of the similarity can thereby be varied.

Since the hash function is not reversible, there is (currently) no constructive method for deriving the string which is to be guessed for the given hash value. As a result, there are a variety of strings to try, which requires appropriate computing capacity. If a node (i.e., a participant of the blockchain network) has found a corresponding string (mining), the new block is added as an element in the chain (blockchain) and, therefore, to the last valid block. For any other node in the network, the correctness is easy to explain by just calculating a hash value.

As a result, a correct linking of blocks to a blockchain can be realized. For the sake of persistence, these chains are now distributed over a large number of nodes, i.e., all nodes have the same basic knowledge. If new blocks are created in individual nodes as a supplement to the existing blockchain, a consensus regarding the change can be reached throughout the network. The cryptographic puzzle serves the purpose of this consensus finding. Once a node has solved a puzzle, the solution is checked and accepted by all involved. Blocks that are still waiting for consensus are organized in a successor list, in which blocks of simultaneously created links are also included in order to re-integrate them into the one global blockchain.

A blockchain with its individual blocks can therefore be managed in a network of nodes. The consensus finding determines which block is adopted as the next element in the global blockchain. Originally, the cryptographic puzzle was used to create new blocks (mining), which is called *proof-of-work*. The difficulty of the puzzle can be adjusted for the sake of different confidentiality and security requirements. A documentation system, such as for distributing power consumption in a smart grid, can work with simple puzzles and therefore also take into account the computing power of the control nodes.

Other types of consensus finding (see Section 2.4) may, for example, consider share certificates in a system. Consensus is reached when the majority of the stakeholders reach the same result (*proof of stake*). Alternatively, nodes may be marked as miners for consensus finding (*umpires*), or lottery-oriented selections may be made. In addition, other possibilities as well as combinations of the mentioned types of consensus finding are possible.

Blockchains can therefore be more easily described as distributed databases that are organized by the participants in the network. In contrast to central approaches, blockchains are much less susceptible to errors and, in particular, prevent *Byzantine errors* (see Section 2.2). However, these systems also bring various challenges along with them. The high degree of redundancy of the data is currently being discussed as particularly critically. By retaining the same data in the network repeatedly, a lot of storage space is needed. Furthermore, the consensus mechanisms often limit the performance of the blockchain. Despite the fact that blockchain technology is still in its infancy, it has undergone several changes in the recent past, most notably its use in a closed business context. Due to the different objectives, there is a fundamental difference between public and private blockchains.

Public blockchains are public systems that anyone with a copy can access. This is not synonymous with automatic reading and writing on a blockchain. It is performed via so-called *full nodes*, which process the approval-free requests of a user. Examples of public systems include *Ethereum* as well as the first generation blockchain behind bitcoins.

Private blockchains describe systems that are only available to a closed consortium, such as organizations. The public character is to be distinguished from the question of the access rights. Public blockchains are often *permissionless*. In the case of private blockchains, access rights are generally administered or restricted to a consortium (consortia blockchain). In most cases, these are approval-based blockchain systems. The most popular example of a private blockchain is Hyperledger.

1.3 Recommendations

Economics and politics are dealing intensively with the challenges and potential of digitization. Developments in the context of blockchain technology will have a major impact on the design and implementation of digital business processes and public processes and, therefore, on social processes. Currently, international standards are set by a variety of initiatives and consortia, making early involvement necessary. This should occur across departments, since it raises issues relating to law, tax, research policy and economics. The following recommendations for action are based on findings of current research work within the Fraunhofer-Gesellschaft, as well as on recommendations for the policies of other countries, such as Great Britain [18] and Australia [9].

At the **political level**, there is currently a lack of a comprehensive legal framework that enables innovation while also protecting the citizens. To achieve this, the following activities are required:

Ensuring legal certainty: Although the transactions in a state-of-the-art blockchain are not manipulable, the use (found to be valid in court) of the transactions or statements stored in a blockchain, such as proofs of origin, is currently unclear. The following has to be reviewed:

- What legal force do the declarations stored in a blockchain possess?
- What functional and cryptographic requirements should a blockchain have for this purpose?
- Blockchain applications are not restricted to a national level, instead supporting transnational processes. Therefore, investigations and the testing of the legal

consequences of transnational blockchains should be initiated, at least at the EU level.

A number of companies are currently developing proof-of-concept solutions for both regulated and non-regulated processes. For these trials to find their way into the new business models, it makes sense to examine the **use of blockchains in highly regulated sectors** (such as energy, finance, medicine and public processes). If necessary and if the pilot tests result in a positive evaluation, the use of the technology should be made possible by means of legislative changes, which then apply across all applications.

These more politically motivated activities should be performed under the condition that an **embedding in the international framework** is guaranteed, so that no singular solutions which are limited to Germany are implemented.

On the **research policy level**, activities are recommended that focus above all on aspects of standardization. Germany is already represented in international standardization through the DIN (ISO/TC 307 blockchain and distributed ledger technologies). This should be actively supported by examining the following aspects:

The standardization and certification of smart contracts: A key feature of blockchain technology is the ability to link transactions with program code to so-called smart contracts. It is expected that patterns and templates will emerge for frequently used applications, as well as marketplaces for smart contracts in the next step. Developing reliable standard building blocks as a result requires:

- auditing and certification bodies to validate their application and process integrity of smart contracts.
- libraries and marketplaces offering smart contracts and, above all, SMEs for use.
- warning systems for the treatment of identified vulnerabilities.

These activities are particularly relevant for the use of the new technology by SMEs. While large companies are able to establish their own departments for the development of smart contracts and blockchain applications, SMEs are reliant on purchasing related services and expertise. Marketplaces for smart contracts are expected to be developed in the future, much like app stores for mobile apps.

Standardization and registration of blockchain infrastructures: In addition to open and widely distributed blockchains, which are primarily used for cryptocurrency, more and more private, access-controlled blockchain applications will be emerging in the near future. It is therefore to be expected that there will be a proliferation of blockchain infrastructures with overlapping application contexts. Therefore, it is necessary to set up a blockchain registry to register and announce blockchain infrastructures in various application areas. The aim of this initiative is to avoid the redundancy of activities and to create synergies. This provides the opportunity to transfer parallel activities to a common blockchain infrastructure. If sharing an infrastructure does not make sense due to technical or business reasons, then it will be necessary in the future to standardize interfaces for interoperability. Only in this way an ecosystem can develop in the long term which enables, for example, the interoperable use of blockchain infrastructures for financial transactions, goods tracking and the quality assurance of production data. Specifically, an **early promotion of**

infrastructures with a blockchain for the research landscape in Germany (e-science) could be implemented.

An **implementation focused on SMEs** would be important in the pursuit of these recommendations. This is mainly due to the fact that, on the one hand, SMEs often work together in value creation networks, exactly where blockchain can fully develop its potential. For this reason, appropriate advisory measures have to be initiated for SMEs in order to develop expertise and to become educated by means of tests and pilots. This may include building and operating SME-focused blockchain infrastructures for a variety of applications. Chapter 3 of this paper details applications and related innovation potentials for possible pilot testing.

2
CLASSIFICATION IN THE RESEARCH LANDSCAPE

Blockchain technology is based on a variety of different individual technology that is combined into a new overall system. These are components from the areas of distributed systems, such as P2P networks, security and cryptography as well as process modeling. These individual components are briefly described in this section in terms of their contribution as well as any necessary research.

2.1
Cryptography

Cryptography is a cornerstone of blockchain technology. It is the foundation for block mining, the integrity of the blockchain itself, as well as the authenticity of all transactions and participants. Without reliable cryptographic primitives, such as hash functions or cryptographically secure random number generators, blockchains in any form would therefore be unthinkable. Blockchain technology, which is still young by the standards of cryptographic research, presents some challenges to science. While most blockchains use proven cryptographic primitives for signing transactions and generating proof-of-works, there is often no statement about the future security of cryptographic primitives. Over time, more and more efficient attacks on cryptographic algorithms will be developed, the computing power available to an attacker is steadily increasing, and previously unrealistic attack scenarios are suddenly gaining relevance, such as *Logjam*[1] and *SHAttered*[2]. In addition, the security of cryptographic systems is far from dependent solely on the choice of appropriate algorithms. Rather, many attacks are aimed at the way it is used and its specific implementation. There are plenty of examples, from trivial implementation errors such as *Heartbleed*[3], which may remain unrecognized over years, to more complex attacks that use system behavior deviations as so-called "oracles" in order to obtain information about cryptographic keys, up to page channel attacks that evaluate (for example) the timing behavior of implementations.

Much of today's blockchain technology neglects these attack capabilities, relying almost exclusively on cryptographic primitives that are considered safe today. However, since blockchain applications in particular are designed for especially long lifetimes – think of a notary function, for example – it is essential that these systems are able to deal with new attacks and possibly broken cryptographic primitives in the future. For secure communication protocols, a selection of several cryptographic algorithms is usually used which are available for each connection setup, so that algorithms that have become unsafe can be easily exchanged. Such "crypto-agility" does not yet exist for blockchains. Rather, recent research has shown [7] that the bitcoin blockchain, for example, is not resistant to possible attacks on some cryptographic components: if it becomes possible in the future to falsify ECDSA[4] signatures, bitcoins could be stolen as a result. If it were possible to invert the SHA256[5] hash function, an attacker could possibly (among other things) calculate the proof-of-work efficiently and take control of the blockchain.

1 *Logjam* is an attack that makes it possible to break the key within an efficient amount of time by downgrading to 512-bit residue class groups during a Diffie-Hellman key exchange.
2 *SHAttered* is an attack that makes it possible in practice to create SHA1 collisions between two different PDF documents.
3 *Heartbleed* is a severe bug in older versions of the OpenSSL open source library, using encrypted TLS connections to extract private data from clients and servers.
4 Elliptic curve digital signature algorithm (ECDSA)
5 SHA (secure hash algorithm) 256 is a special cryptographic (i.e., collision-resistant) hash function.

Measures against such attacks – should they ever become possible – are extremely complex. Although the protocol can introduce a new hash function while backwards compatibility is lost, old blocks with block hashes from the old, insecure hash function have to be preserved according to the design. As a result, the new clients would now have to solve two proofs-of-work instead of just one.

In this regard, science is therefore mainly faced with the following challenges:

1. The development of cryptographic primitives that are also resistant against future attacks, such as by quantum computers.

2. The design of blockchain protocols that support crypto-agility and still provide security guarantees for transactions in the event of effective cryptographic attacks on individual primitives.

3. The development of procedures that correctly implement critical operations in blockchain protocols in a demonstrable manner in order avoid fatal implementation errors, as have frequently occurred in OpenSSL.

2.2
Consistency and scaling of distributed systems

Distributed systems included all those systems that use multiple computers in order to complete a joint task. An example of such a use is the transaction systems of a stock exchange or flight booking systems: In such cases, several computers are necessary for the sake of load distribution. At the same time, however, it would have to be ensured that a transfer were performed precisely once, similarly to the procedure with a database transaction. It is important that is does not matter whether the systems are working correctly at any particular time: A software error or hardware defect may not change a transaction.

This problem is known in computer science under the keyword "Byzantine generals" [12]: Imagine a city that is surrounded by several armies which are each under the leadership of one general. The armies are only able to take the city with a joint attack. In order to coordinate the attack, the generals send messengers with messages to the other armies.

In this thought experiment, it is easy to reconstruct various fault conditions from distributed systems: What happens when a messenger is intercepted on the way? What if a messenger changes the message maliciously? Or by chance? A "byzantine fault tolerant" system is one that remains stable despite such errors and, for example, guarantees the transaction properties. The blockchain is an example of such a system.

However, the highly distributed P2P nature of the blockchain pays for this robustness with time delays. In the bitcoin blockchain, for example, it takes an average of ten minutes to find a block – and only after six blocks can a person really be sure that his own transaction has been correctly posted to the blockchain. To compensate for this disadvantage, this aspect of the blockchain could also be centralized again.

To do so, the P2P network would be replaced by a smaller number of service servers which are in contact with each other, like the generals in the above analogy. These servers communicate with each other and provide a sufficiently redundant execution of the blockchain. In order to protect against false messages, message losses, etc., methods such as *Raft* [13] can be used. In addition, this partial centralization enormously simplifies the installing of updates and bug fixes.

In the corporate environment, blockchain technology offers a lot of opportunities. However, aspects such as compliance or timely bug fixes are difficult to integrate into the highly distributed structure of the current blockchain systems. It will be a task for the future to adapt these systems such that they meet the needs of the respective enterprise.

In terms of distributed data management, the blockchain concept relies on the storage and replication of all managed transactions, i.e., of the entire dataset in all participating nodes of the P2P network. The lifetime of a blockchain therefore continuously increases the replicated data, which leads to a critical assessment of scalability. In order to avoid the rapid growth of the blockchain, large data objects are not stored in the blockchain; instead, only the essential transaction information and, if necessary, references to the associated data objects are primarily stored there. These are stored in an external database, provided that the data object is to be retrievable directly via the transaction. Alternatively, instead of a reference, a fingerprint of the data object may also be stored in the form of a hash value. In this alternative, the hash value can be used simultaneously for retrieval from an external database as well as for verifying the integrity by means of comparing the fingerprint of the reconstructed object with the fingerprint that has been stored in the blockchain (see also Section 3.3).

However, when using a blockchain for the management of high frequency transactions (such as may occur with sensor data in the Internet of things, for example), even this method can prevent the blockchain from growing continuously and, therefore, that the computing and storage capacity requirements of the nodes in the distributed network system grow. For this reason, further research is needed in order to avoid that these technical requirements lead to unwanted centralization. One possible solution is to consolidate the blockchain on the *unspent transaction output* (UTXO), which is a form of balance formation that can reduce the size of the blockchain by deleting transactions which no longer help to determine a user's credit. Another possible solution is to *shard* the blockchain, whereby the nodes only manage parts of the blockchain but still maintain the integrity of the entire chain. Despite these initial approaches, scaling challenges in terms of size and transaction throughput provide interesting future research potential.

2.3
P2P networks

Peer-to-peer networks (P2P networks) only have peer-to-peer nodes, which means that, unlike in the case of client-server architectures, all participants in the network can perform the same functions. As a result, P2P networks are very resilient to failure, since all computer nodes can perform all the functions which are necessary for the network to operate. Furthermore, due to the structure of a P2P network, aspects of load sharing and self-organization are quite easy to solve. As a result, large P2P networks achieve very high throughput, such as based on the BitTorrent protocol and the high number of connected computer nodes [15].

At the same time, however, this architecture also leads to greater complexity. The basic challenges of P2P networks are [4]:

- Intentional manipulation: Nodes in the P2P network do not necessarily all have to pursue the same goal and may seek to maliciously influence the functioning of the network in their favor. If the network is used for payment, for example, a node could try to simulate a payment which actually did not exist. Such incorrect information has to be detected and rejected by all other nodes.

- Erroneous information (such as software errors or communication problems) can lead to problems in the network just like deliberate manipulation can. These have to be detected and processed accordingly, just like in the case of manipulation attempts.

- For many applications, it also has to be ensured that a transaction in the P2P network is executed precisely once and completely, i.e., that is has the properties of a database transaction.

Blockchain solves these problems by ensuring a consensus. In contrast to highly complex consensus algorithms, such as *Paxos* [14], blockchain assures the integrity of the information within the blockchain by constructing the data structure. This design solves all the challenges described above.

A disadvantage of a P2P network, however, is that the program logic is stored in all participating computer nodes. If an error is found, for example, then all of the computer nodes have to install an update[6].

2.4
Consensus building and validation

The technique of consensus building is another cornerstone of blockchain. The methods used are based on concepts that have long been studied in the context of distributed networks [3] and distributed systems [12]. The most well-known method currently used by a blockchain implementation is the proof-of-work of the bitcoin blockchain. The actual proof-of-work concept was already proposed in 1993 to curtail junk e-mails [5]. It is based on an asymmetric approach in which a service user (i.e., the e-mail sender) has to perform work that can be easily checked by a service provider (i.e., the e-mail network provider). In the blockchain context, the users are the *miners* that laboriously compute the proof-of-work, and the providers are all the *nodes* that can easily verify whether the successful miner has duly computed the proof-of-work. In the bitcoin blockchain, the proof-of-work algorithm is based on the method presented by Adam Back as *hashcash* [2] [16]. The goal of the algorithm is to find a number (*nonce* = number used only once) which, in combination with the new block that is to be appended to the already existing blockchain, results in a hash value that consists of a certain number of leading zeros. If several miners simultaneously find such a value and attach it to the blockchain, this results in a branching of the blockchain when the new block is distributed to all nodes of the P2P network. If three nodes find a matching nonce almost at the same time, for example, adding the new blocks would divide the existing block chain into three branches. To consolidate this division, the majority decision applies: the branch is selected that represents the longest chain, i.e., represents the greatest number of the transactions or most of the work. The other two blocks expire and the transactions which are contained therein but are not contained in the attached block are again included in the pool of transactions that are yet to be validated.

This proof-of-work method is CPU-based, i.e., the computational speed of the nodes has a significant influence on who resolves the puzzle and finds a matching nonce value. Since miners are rewarded with new bitcoins for finding the nonce, a competition is created that leads them to invest in more and more computing power. This would reduce the time it takes to find a valid nonce, but it contradicts the bitcoin network rule that a new block should only be generated approximately every ten

6 In the case of Ethereum, for example, a protocol error caused the incorrect debiting of account balances that could only be remedied by a hard fork and a non-backwards compatible software version [10].

minutes. This is because the successful miner is rewarded with newly created bitcoins. If the intervals in which new blocks are generated were shortened, the money supply would increase too fast. For this reason, the difficulty of the puzzle is always increased when the time is shortened by newly added computing capacity. For the miners who operate the computer nodes, this means increased effort and less chance of success. Since the effort, in addition to the investment in the computing power, essentially consists of the consumed energy, this approach is not useful for all blockchain applications. This is especially true for private blockchain solutions, whereby such competition is not required. For this reason, alternative proof-of-work methods have been developed that are based on either a respective memory or a respective network. With memory-based approaches, the puzzle cannot be solved by computing power, rather by a corresponding number of memory accesses [1].

An alternative method which is particularly relevant for private blockchains is the proof-of-stake method, whereby the nodes that can validate a new block are chosen according to their share of the cryptocurrency [11] or via a random procedure [21]. A combination of proof-of-work and proof-of-stake procedures is also possible.

The selection of the most appropriate method depends on the specific application and the use of the blockchain solution as private vs. public or free of approval vs. subject to approval. Another important aspect is the scalability in terms of the number of transactions, especially in applications concerning the Internet of things. This results in the following research questions, among others:

- Which consensus procedures offer the best solution in terms of security, costs, scaling and performance, depending on the field of application?
- What is the cost/benefit calculation with different weightings of requirements?
- Which consensus procedures are safe for the future, taking into account increasing computing power and new technology?

2.5
Smart contracts

A blockchain enables not only the decentralization of transaction management, but also the automation of processes, regulations and organizational principles. The transactions can be supplemented by rules for preserving consistency and then become so-called *smart contracts*. They specify what to check in a transaction and what follow-up activities are to be initiated. Frequently mentioned examples of smart contracts are electronic door locks that automatically check whether the user has paid the user fee and still possesses the necessary legitimacy, such as a driver's license.

Through smart contracts and the associated automation, many processes can be radically improved as part of a re-engineering process and can in some cases also be facilitated by certified inspection bodies if the consistency of the information is ensured by a smart contract and audit-proof storage. Classic principles of the re-engineering manifesto [8], such as *capture only once*, can therefore be implemented in a natural way with blockchain as an enabler. Once information has been confirmed, it is documented in an audit-proof manner and can be integrated in a variety of contexts. As a result, from a technological point of view, blockchain is a natural tool for process optimization. If, for example, it is only possible to upload a video to a community platform if the corresponding audio rights are available, the entire supervision and monitoring processes can be omitted. However, this consistency is easy to maintain through smart contracts.

Blockchain technology therefore not only has diverse effects on the processes, but also on structures of governance that can significantly change the distribution of tasks between process participants. This, in turn, raises the question of new business models for the new value chain after the process has been redesigned.

Because of the disruptive potential of the blockchain, traditional forms of process optimization appear to be rather unsuitable. A revival of classical re-engineering methods seems possible, since they have analyzed processes from a strategic perspective and as customer value. Re-engineering also takes into account the role changes of the stakeholder. Since process modeling needs to be integrated with the development of new governance and business modeling structures, questions such as the following arise:

- Previous modeling languages for processes are highly control-flow oriented. The question is how to integrate new forms of certification by regulatory authorities into the modeling methodology. Can this be done using new role concepts or can process patterns in the sense of control flow patterns offer alternatives to new governance in libraries?
- How can value chains from process modeling be combined with those of business modeling? Value-chain-oriented methods from business modeling, such as e3-Value, are highly process-oriented but neglect the various stakeholders and the value proposition for the customer.
- What could a method and a modeling language look like with which the necessary social, economic and industrial achievements are made sustainable through innovative processes on the blockchain?

2.6
Trustworthiness/security of smart contracts

Smart contracts make a blockchain more than just distributed secure storage and make possible the automated and trustworthy modification of information in the blockchain. For example, smart contracts can be used in bitcoin to process various types of transactions, such as *escrow*, i.e., to realize the fiduciary deposit of data. While smart contracts in bitcoin consist of only a few operations and cannot handle loops, the Ethereum blockchain offers a "quasi-Turing-complete" language that costs "gas" to run in a dedicated virtual machine. The Hyperledger blockchain goes further and allows the execution of almost any program. These are called chaincodes, which can be written in various high-level languages (such as Java or Go) and are run by trusted "validating peers". During execution, the chain code has access to the information stored in the blockchain and can read it or store further information. Furthermore, during the execution, the chaincode is isolated from the rest of the environment only by docker containers, i.e., the execution does not take place in a virtual machine, but instead directly on the processor of the peer.

The correctness of smart contracts is of utmost importance, since, in contrast to desktop or web applications, for example, continuous updates of smart contracts are not readily available. This means that once smart contract code has been entered, it cannot easily be revised without questioning the integrity of the data stored in the blockchain. In fact, in the past, attacks on smart contracts have frequently been reported, some of which were made possible by hard-to-recognize programming errors (unchecked-send, reentrancy, solarstorm). In addition, though, the execution environments for smart contracts are also partially uncertain. For example, Hyperledger

cannot currently guarantee that chaincode terminates[7]. Since the executing environment can at the same time use the validating peer's unlimited CPU resources, smart contracts can easily be used as a denial-of-service (DoS) attack on the peer. Furthermore, chaincode, for example, is not limited to communication with the blockchain, but can also call up external services. As a result, harmful smart contracts are also conceivable which, for example, send spam or act as bots within the blockchain.

When using smart contracts, two things therefore have to be ensured: on the one hand, the smart contract itself has to be correct and secure against attacks such as *reentrancy*. In practice, this is not trivial to ensure, as the DAO attack has shown. On the other hand, it has to be ensured that no malicious smart contracts enter the blockchain. This is especially true for blockchains with powerful smart contract languages, such as Hyperledger and Ethereum. While Ethereum is taking the first steps in the right direction in supporting the formal verification of smart contracts through the *why3* framework, such procedures are still too cumbersome for most developers and require too much background knowledge in order for the procedures to be used in a meaningful way.

In general, there is still a high need for R&D in the area of secure smart contracts – both in using formally verifiable languages as well as in assisting developers and in the validation of code prior to inclusion in the blockchain.

2.7 Business models

Due to the specific nature of blockchains – especially distributed consensus building, the digital transfer of values, automation and irreversibility – the technology has, on the one hand, the potential to challenge entire business models of many organizations and institutions. On the other hand, it also offers the possibility of new business models that would not be reproducible without blockchain, or at least not in an economical manner.

The potential of the blockchain is recognized for a variety of contexts and applications. At the same time, it is currently unclear what structural characteristics of business models particularly benefit from the advantaged of blockchain and how they can be economically viable.

Against this background, numerous questions arise for academic research concerning business models and the cost-effectiveness of blockchain solutions:

- What are viable applications for blockchain technology – even from an economic perspective – and how should they be designed?
- What are properties of business models – abstracted from the specific application – that can benefit from a realization with blockchain?
- How can the impact of a blockchain implementation on established business models be predicted – such as in the event of the elimination of intermediaries?
- How can the corporate benefits of blockchain solutions versus traditional implementations be determined?

7 See sachikoy: there is no mechanism to abort chaincode even if it has an infinite loop; 2016-0616, https://github.com/hyperledger-archives/fabric/issues/2232 (last visited: May 23, 2017)

- How can blockchain business models be modeled and implement in an economical and meaningful manner?
- Beyond individual companies, what impact will the technology have upon existing industries or the economy as a whole?
- What opportunities and risks arise for the economies of Germany and the European Union?

A scientific answer to these questions would help to unlock the potential of blockchain in specific real-world scenarios. In many cases, today's application scenarios do not go beyond the prototype status. Only a well-founded analysis of suitable business models and their cost-effectiveness will help blockchain to make a breakthrough in viable application scenarios.

3
APPLICATIONS

Currently, most of the practical blockchain application scenarios are without doubt related to the financial sector. An overview of specific blockchain solutions makes it clear that various projects in this field can be assigned to the following areas of application.

- Cryptocurrencies: Blockchain application as a transaction log for various cryptocurrencies, such as Bitcoin (BTC), Ethereum (ETH) and Monero (XMR).
- Business networks: Blockchain applications in the area of smart contracting and data exchange, such as Ethereum (smart contract applications), Hyperledger and MultiChain.
- Banking: Blockchain-inspired applications in financial transactions, such as Corda and Ripple.

Blockchain technology is used by various FinTechs. The financial services provider Bitbond, for example, received a license from the German Federal Financial Supervisory Authority (BaFin) at the end of 2016 and handles the lending business between individuals (P2P lending) by means of blockchain technology. R3 is a consortium of leading worldwide financial institutions that is working on the implementation of a block-chain-based system for managing financial transactions between financial institutions (Global Fabric for Finance). In this process, they rely on the blockchain solution *Corda*. *Ripple* provides a communication protocol for banks based on the blockchain technology similar to the SWIFT (Society for Worldwide Interbank Financial Telecommunication) protocol.

Blockchains can be used in all areas that involve capture, proof, or transactions of any kind of contract or object [9, 11]. IBM, for example, has recently presented the blockchain-based trade register. *Everledger* is based upon an exceptional application scenario: The company creates or manages digital documents concerning the origin, identification, and ownership of diamonds and writes them into a blockchain with the goal of limiting fraud in the diamond trade.

In the areas of B2B trading and supply chain management, the company *Skuchain* is developing various blockchain-based solutions, such as for the real-time tracking of invoices and transactions as well as the documentation of component histories in the supply chain [12]. Blockchain is also used in trade. *Walmart* is developing a blockchain system for tracking food testing. The consulting firm *Gartner* predicts that the current hype surrounding blockchain has nearly reached its peak and that the number of blockchain implementations will skyrocket over the next five years [10]. The following sections take a closer look at some of the application areas and industries for these solutions.

3.1
The Internet of Things

An essential element of the Internet of Things (IoT) is the digital networking of all physical smart objects via smart services. The aim is to improve the quality of the interaction between man and machine or even between machines. Since a central coordination of the Internet of Things would probably be almost impossible, it also aims at a far-reaching autonomy of the intelligent objects. This autonomy can be supported in several manners by blockchain technology.

For logistics as one of the main application domains, this means that resources and goods network with each other, exchange their statuses and negotiate specific interactions in the interests of optimal added value. The resulting value-adding activities have to be tracked and stored transparently for all involved actors. It does not matter whether it concerns internal company processes (e. g., determining the utilization of resources, traceability in the case of a quality defect, ecological footprint or process cost calculation) or cross-company processes (e. g., cost allocation, billing, proof of use). In any case, the value added processes that have been performed have to be documented and the relationship between the goods and the utilized resources and work equipment have to be made available, in a form that cannot be manipulated, to all those involved. In the case of the proof of use of a product or the ecological footprint, this also applies to the customer who has a particular interest in non-manipulable information.

In this regard, in this basically decentralized system, blockchain can offer an approach that can replace a central authority which is difficult to implement and which is essentially not in the interests of those involved. A great challenge in this regard lies in the (secure) connection of the physical objects with their data (which, for example, is collected by sensors) and the corresponding entries in the blockchain. It is important to ensure that virtual entries (in the blockchain) and physical objects (such as goods) are uniquely linked with each other and can be assigned.

With the IoT, smart contracts offer the possibility of machines reaching agreements that are guaranteed to be complied with in both directions. In line with the Internet of value, machines can then bill their services directly to their user and save earned money decentrally in an *e-wallet*. Contract and billing can also come about if a machine is not connected to the Internet at that time. They will be synchronized later via the blockchain.

For example, future business models would be conceivable in which manufacturers let autonomously operating machines (e. g., autonomous vehicles) offer their services (e. g., taxi rides) completely free of charge. Machines then earn their money directly (e. g., by transporting people), report maintenance requirements independently and bill directly in both directions. Surpluses are finally posted to the manufacturer. Even the already politically discussed taxation of the work of robots would be easy to realize. Like human workers, part of the machine's income would be diverted to the state and, therefore, to the general public.

3.2
Smart grid

The smart grid is essentially an instance of the Internet of things and presents far-reaching challenges due to the complexity of the electricity grid. The energy sector is currently being shaped by two key trends: First, with their volatile supply, renewable energies require improved coordination of supply and demand in the grid. Second, this supply is often no longer – as in the past – at a few, central points (large power plants), but rather decentralized in the area. This decentralization is not only spatial, but also organizational: Instead of less power plant operators, every homeowner with a photovoltaic system can participate in the electricity market today.

Specifically, for example, it is being discussed that *prosumers* of used or self-generated electricity no longer trade with their respective electricity provider, but instead with others prosumers in the net. In the sense of the Internet of Things as described above, this could even be directly related to individual devices; for example, a photovoltaic system could supply and bill its electricity directly to an electric car. Due to the limited

credibility of such arbitrary actors in a decentralized electricity market, blockchain technology provides an ideal basis, thanks to its ability to transfer value.

Alternatively, though, centralized solutions would continue to be available. For example, distribution system operators could coordinate decentralized trade and, thereby, represent a decentralized center of trust. It therefore remains to be seen to what extent solutions in the smart grid will be used in the well-developed and heavily regulated electricity market or to what extent they will be used particularly in other or more specific application scenarios.

3.3
Proofs of origin

Providing, reviewing and preserving proofs of origin (provenance) today represents a significant economic factor. Not only are auditing firms, auditors and certifiers affected by the potential for change in a blockchain: so are manufacturers with regard to tracking their products.

Systems such as Everledger make it possible to track owners as well as the change of ownership, such as regarding diamonds. Everledger documents all ownership-related transactions for each diamond. As a result, the ownership history can be traced beyond doubt back to the registration in the system. The possibility of identifying diamonds is advantageous: Due to its optical behavior, each diamond is uniquely identifiable, similarly to a fingerprint. When a diamond is examined, the fingerprint can be used to verify whether it is known in the blockchain, enabling the ownership to be clarified. This service is of interest for a variety of business partners, such as banks, insurance companies, diamond dealers as well as police and courts. Everledger builds on the unique identifiability and value of the product.

Comparable proofs of origin are also needed for other industrial sectors and product types, though. Firstly, in the case of product approvals, it has to be proven that certain conflict minerals (such as tin, tungsten or tantalum) were not used in the production process. On the other hand, the use of manufacturer-certified spare parts is of interest in order to ensure that, for safety reasons, no counterfeit components are used. Both can be based on a clear identification of the products or audit-proof duplication of the bookkeeping. At the core, it always has to be ensured that the origin of the products and raw materials is clearly traceable.

When transporting dangerous goods, for example, each vehicle is to be supplied with extensive documentation regarding transport containers, vehicle characteristics, training, etc. With smart contracts, the regulations and provisions in the sense of an electronic contract management can be mapped, i.e., rules and processes are formally described and automatically monitored. Since, according to newly established guidelines of the supervisory authorities, the transport documents are now to be managed in digital form and are readable by various stakeholders, a closed system of information and processes for transporting dangerous goods is obtained, which can always show that the legal requirements for each transport have been followed. In addition, international transport chains can check national regulations while at the same time standardizing safeguards in order to comply with the minimum requirements in each country.

Personal proofs of origin also play an important role in the administration of personal certificates. The digitization of the application process means that relevant certificates and documents are exchanged digitally and a later review of the originals hardly takes place. A certificate blockchain can ensure that submitted certificates are not subsequently manipulated. For this purpose, it is necessary that the issuers of such certificates (universities, further training institutes, Chamber of Industry and Commerce, TÜV, etc.) register a digital fingerprint of issued documents in the blockchain. Owners of the documents can use this entry to document the integrity of a submitted document, which creates additional confidence in the correctness of an application or even of seals of approval.

3.4
Supply chain management and purchasing

Supply chain management is an interesting field of application, since the diversity of value creation partners consisting of suppliers, manufacturers, retailers, logistics and financial service providers, between whom different performance agreements exist, need technology for the secure exchange of data against the background of increasing digitization. The digitization efforts in the context of the IoT also lead to many new possibilities of smart process control in supply chain management and, particularly, in financial supply chain management.

While today we seem to have reached the limit of what is possible in the field of the physical service delivery of logistics processes in the supply chain by means of automation, the latest hardware and software and intelligent planning concepts as well as smart processes, financial processes in the supply chain are still too slow and are therefore decoupled from the actual service creation process. The reasons for this can usually be attributed to manual and error-prone processes. Today, more than 60 percent of B2B transactions are still based on paper invoices. By using blockchains, transactions can be handled independently of invoices via smart contracts. This technology also allows easy integration and secure networking between different supply chain partners. Figure 2 illustrates a simplified blockchain-based supply chain network made up of various partners.

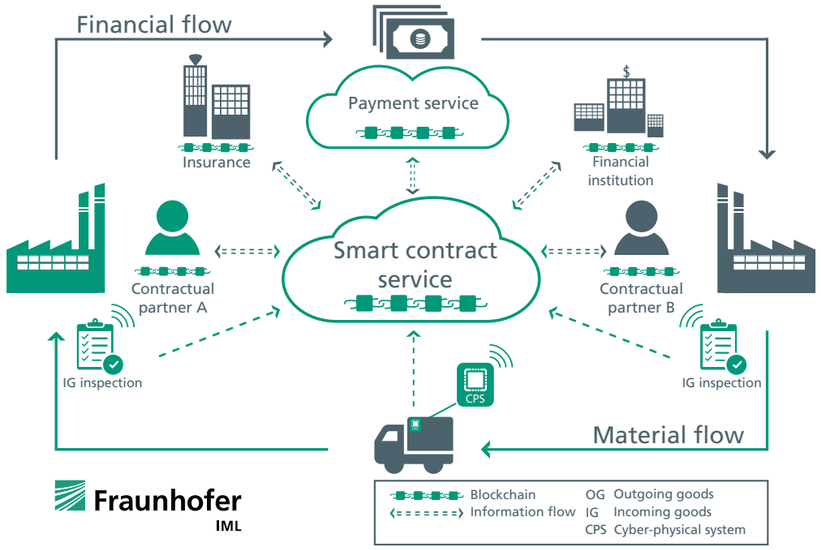

Fig. 2: Blockchain-based supply chain network

The blockchain acts as distributed data storage and publicly and irrevocably safeguards all relevant information for the smart contract. Based on this information, the smart contract (as the executing computer program) verifies compliance with the respective content of the contract and independently authorizes financial transactions in the fulfillment of certain contractual conditions. In combination with the use of decentralized control units[8], logistics objects in the supply chain network can autonomously make scheduling decisions and assign orders independently.

In addition to autonomous scheduling decisions and independent transaction processing, smart contracts offer great potential for increasing the efficiency of processes, especially in operational and strategic purchasing. For example, orders can be executed autonomously, and value-added parent trees can be created across various levels of the supplier chain (Tier 1-n) for quality assurance and supplier development via the blockchain. The gain in transparency for manufacturers would be enormous. There are already examples of how leasing agreements can be monitored using these smart contracts. If the lessee fails to pay the leasing fee on time, the vehicle can be blocked or further driving can be prevented through the system.

3.5 Medical engineering

Various applications of blockchain and smart contract technologies are conceivable in the field of medical engineering. Although no specific application scenarios have been implemented and published yet, research interest in this field has already been aroused, driven by the value proposition of solving fundamental problems on the way to data-driven, personalized medicine in an environment of highly sensitive data. In the age of digital medicine, more and more health-related data exists in different systems. This includes sensor data (e. g., from wearables) as well as radiological images, clinical information from electronic health records as well as highly sensitive data, such as the results of genetic tests.

On the other hand, it is a requirement of modern preventive medicine to evaluate such data across the population. The classical method of modeling cannot be followed in this environment, since data of this kind cannot be collected and provided in a centralized manner. One possible solution consists of mechanisms that allow the owner of the data to have transactional, auditable control over the data's use. This is precisely the value proposition of blockchain technology.

Not all blockchain characteristics are needed in the field of medical engineering. For example, it is not absolutely necessary to decentralize the verification. According to the prevailing opinion, at least three major technical challenges still have to be mastered:

1. **Seamless** monitoring of **data usage**: It has to be demonstrably ruled out that data usage occur outside of the system. This may also require the certification of secure hardware.

2. **Group- and person-specific usage permission**: It has to be possible to limit the use of data to specific persons or institutions or to specific parts of the data.

3. **Complete decentralized data and event logs**: In a scenario in which data is stored decentrally (in hospitals, insurance companies, mobile devices, etc.), data has to be transferred between systems. Securing transmission against abuse is a major challenge.

8 see Fraunhofer IML: SOFiA – Smart Objects und Smart Finance Ansätze; http://www.sofia-projekt.de (last visited: May 24, 2017)

In all three areas, there are projects and approaches that could provide a basis for creating a novel approach to personalized data-driven health management.

3.6 Financial sector

The financial sector is currently the sector with the largest activity in the blockchain area. However, many established financial institutions are just beginning to harness the potential of blockchain. While it is not infrequently emphasized that blockchain could, in theory, completely replace financial intermediaries, these institutions are currently putting much of their energy into improving existing financial systems and services through the use of blockchain technology. In order to provide an assessment of the impact of blockchain on the industry, selected examples of blockchain applications in the financial sector are analyzed below.

Today's payment processes involve several intermediaries, such as banks, clearing houses and central banks, and are very resource intensive. In addition, due to the many intermediaries and different systems as well as reasons associated with coordination and cost, settlement processes do not take place continuously, but instead only a few times a day, causing noticeable time delays. Blockchains theoretically have the potential to eliminate these time and cost disadvantages. The finance industry is focusing primarily on international transfers, in which particularly high fees are currently incurred. In addition, shorter settlement times would reduce the foreign exchange risk involved in international transactions. In addition, blockchain-based payment systems can increase security and privacy, since payments are based on the push-principle: customers can actively initiate transactions without providing details such as bank information. Advantages for merchants may include the prevention of fraud (due to the transaction irreversibility that is inherent in blockchain systems). Furthermore, there are low processing fees as well as cost and risk minimization, since customer payment information does not have to be stored.

Since transaction processes in capital market trading involve a large number of actors, data has to continuously be reconciled and replicated as part of validation processes, resulting in high costs, long transaction times and operational risks. Accordingly, a promising field of application for blockchain is above all seen in the settlement of securities transactions. Using a blockchain solution could significantly decrease the cost and complexity of transaction handling and reduce the processing time to minutes or seconds, since the parties trade directly with one another. Shortening the time span reduces both operational and counterparty risk, potentially reducing the capital requirements for banks. The credit and liquidity risk could effectively be eliminated, since the functioning of blockchain systems involves trading being subjected to the prior possession of the corresponding funds.

Blockchain technology also allows for bills-free transactions in conjunction with the use of smart contracts. While paper invoices that have to be checked, confirmed and forwarded by means of lengthy manual processes form the majority of billing in the B2B area today, blockchains secure the contract contents (service level agreements) and smart contracts supervise the contract execution. The transaction belonging to the performance task can then be triggered automatically. The transaction confirmation is also stored in the blockchain. These automatic transactions that are decoupled from the billing process are called smart payments.

Especially in the financial sector, great potential for blockchain is also seen in the area of compliance. In this context, two possible uses of the blockchain are being discussed: firstly, as a central register for consolidated accounting and, secondly, as a *consortium blockchain* for customer data. Banks currently maintain a variety of different account books for different purposes and implement various measures to prevent accounting misconduct. This typically involves performing various data integrity processes and sharing the responsibility for including financial data in the books. By using blockchain concepts, these processes can be largely automated, since blockchain enables the trusted consolidation of individual account books into one data model. The avoidance of the double-spending problem in blockchain systems is especially useful in this regard. Manipulation in accounting, such as the backdating of contracts to other periods, can be prevented by means of the irreversibility and reliable timestamping of transactions. The fulfillment of various laws and regulations for money laundering prevention, such as *Know Your Customer* (KYC), involves high costs for financial institutions and delays transactions, sometimes decisively. In addition, KYC processes are performed individually in different financial institutions. An industry-wide customer registry based on a blockchain system could eliminate the multiple overhead of KYC reviews and facilitate the encrypted transmission of customer data. In combination with the use of smart contracts, various aspects could also be automated.

3.7
Media industry

Cryptocurrencies like bitcoin or Ether offer approaches to alternative remuneration models and fuel fantasies in the media industry. In times of transparent data streams, the omnipresent metadata chaos in the music industry, with its fragmented rights (including their local characteristics), seems above all to be the starting point for focusing on blockchain. In light of all the unsuccessful attempts so far to introduce uniform registration and licensing standards within the industry, the various stakeholders are relying primarily on the promises of this technology, especially after the end of Global Repertoire Database activities (July 2014, [6]).

Unlike in the classical origin histories, even the smallest portions of the media distributed in the market (music pieces, films, etc.) are provided with IPs by many individual claimants, which makes traceability and authenticity checks virtually impossible for the claimants themselves.

In all considerations of the market participants for an initial use of blockchain, the non-transparent license streams in the digital business models play a particularly large role. In the case of the major market participants, due to unidentified rights holders, about to percent of the licenses[9] from the so-called *black boxes* retain their intermediary roles between consumer and creative. This is in contrast to the situation in the financial industry, where such payments go into government funds, such that a pressure to bill properly is always maintained.

In order to use blockchain technology as an alternative solution for all actors and, above all, for a global, transparent and timely remuneration of creative individuals, an intensive discussion among all key participants and stakeholders and their alignment with each other is required (*stakeholder alignment focus*). The objectives of this exchange are cost analysis, the development of a roadmap for stakeholder collaboration on standards, and the conduct of social impact discussions in order to support the

9 Fair Music: Transparency and payment flows in the music industry (Rethink Music, a project of Berklee Institute of Creative Entrepreneurship 2015)

technology as well as to understand possible regulators and regulatory frameworks. In this process, the Fraunhofer-Gesellschaft can help players to keep an eye on the most important transformation potential of blockchain: reducing the need for intermediaries to autonomously execute transactions. Among other things, this means:

- Establishing agreements in a shared platform with a guarantee to execute them, based on mutually agreed terms and with a limited number of required countermeasures.
- Eliminating the need for assistance in performing license transactions.
- Reducing risk due to mistrust of the assets or obligations of the parties.
- Abolishing intermediary roles and their potential for conflict in the resolution of current and emerging digital business models.

The successful use of the blockchain promises, above all, the creation of shared, transparent repositories for information (metadata, digital content, license ownership) that is shared by multiple partners. This occurs on the basis of the definition of all relationships of those who have write authorization to all participants and their shared transactions (licensing, processing) for a licensing system which is controlled by a small number of authorized market participants and operated in a completely transparent manner. All intermediaries operating individually or in combination within the exploitation chain benefit from the traceability and automation of inter-dependency transactions in a blockchain-based system and are therefore able to accommodate new business models of the partially endangered facilitator role and of the disruption.

3.8
Public sector

For the public sector, blockchain technology is both a risk and an opportunity. The digitization of administration has so far been characterized by accelerating existing processes or making them more efficient. Blockchain technology adds a new dimension by replacing state-organized functions with privately organized ones. At the same time, the use of blockchain technology offers the potential to strengthen transparency and trustworthiness in administrative processes. Blockchain also offers the opportunity to simplify processes for intra-administrative communication, especially for administrative processes across various levels.

In many cases today, actors of the public sector perform the role of intermediaries. The public administration maintains registers to document ownership structures, while notaries, through their special position of trustworthiness, ensure ownership transfers. In addition, the state serves in many situations as a trusted third party, such as when it comes to confirming identities of persons or things or verifying the authenticity of documents.

Accordingly diverse potential applications in the public sector are being discussed, as shown in Figure 3 on page 30. The spectrum of the current discussion ranges from e-payment, transparency and openness, publicly managed registers and management of ownership structures, guarantees of origin, verification and confirmation services, mapping of digital identities to securing electronic elections. These are often conceptual considerations or prototypes. However, there are also examples in which the technology has been in productive use for several years. One example is Estonia, which has been protecting the integrity of medical documents with blockchain-like

technology[10] for several years. Since 2015, the country has also been offering a blockchain-based emergency service with its e-residency program. In addition to Estonia, many other countries are working intensively on the technology and developing strategies for using blockchain in administration, including the United Kingdom, Dubai and the United States. In the process, a variety of application scenarios are being discussed.

Fig. 3: Application fields of blockchain technology which are frequently discussed on the international level [17]

The obvious application of e-payment is just as trivial as it is easy to implement. An example can be found in the Swiss city of Zug, where bitcoin is accepted as payment for administrative fees. A service provider that exchanges bitcoin in Swiss francs on the same day reduces the risk of excessive price fluctuations for the administration.

The other areas of application are more visionary, but are also associated with more complex process adjustments. Blockchain is mentioned with particular frequency in the context of registers and the transfer of ownership. Its ability to document transactions verifiably, transparently and immutably comes very close to the requirements of classical registry management. The reasons for using blockchain technology in this context may vary. It is interesting for those regions where classical state structures for registering or trust in them are lacking. Wherever state structures are already established, the technology can make the transfer of ownership process even more transparent and, if necessary, faster.

In addition, the technology can also be used for intra-administrative cooperation, such as to check whether certain data or documents are stored at an administrative department or not. Furthermore, via a blockchain, it is possible to secure the integrity of data and documents which, at least from a user perspective, can be a lightweight alternative to digital signatures (see also Section 3.3).

10 Specifically: keyless signature infrastructure (KSI)

Another application is e-voting (electronic voting) or even I-voting (voting over the Internet). In such a context, each voter generally receives a coin or token that represents his vote. Each candidate gets a receiving address (comparable to a wallet). The election itself is represented by a transaction of the token to the candidate's receiving address. For the field of parliamentary elections, though, discussion concerning the use of technological aids is very controversial in Germany.

In the German administrative landscape, blockchain technology has only arrived in specialist circles so far. The public administration in Germany has been undergoing profound changes for several years, due to an increasing number of tasks combined with increased requirements and ever-tighter budgets. For a long time, digitization has been seen as a way out of this dilemma. Due to its decentralized nature, blockchain technology therefore offers an interesting perspective for the federal structure of the German administrative landscape.

Many of the internationally discussed application scenarios in the public sector are accompanied by a number of new challenges. Building and running a blockchain are not trivial and require experienced professionals, including cryptologists and computer scientists. In addition to a variety of open technical points, there are also fundamental questions involved. Classic intermediaries create trust through organizational measures. Intermediaries in the public sector are subject to special requirements with regard to correctness and trustworthiness. Blockchain technology replaces this organizational trust with confidence in technology and its cryptographic processes. In this context, it has to be considered in each case whether the use of blockchain is reasonable and sustainable in the long run.

3.9
Legal sector

On the one hand, blockchain can fundamental challenge the validity claim of law while on the other hand opening up new means of law enforcement. The decentralized and usually pseudonymous architecture of the networks plays the decisive role in such a process.

The overwhelming majority of the legal system is organized in a technologically neutral manner. The fact that a particular transaction is handled using blockchain technology usually does not affect the legal nature of the transaction. There are also exceptions to this principle, however.

Open blockchain networks generally operate globally and readily allow cross-border transactions. Coupled with pseudonymous structures, this often makes the traditional law enforcement approach virtually impossible. Blockchain-based networks are therefore bound to a very limited extent to regional legal systems.

Classical regulatory law is based on the assumption that it is possible to define a specific addressee and, if necessary, to be able to get hold of him. This assumption is entirely placed in question by both the decentralization as well as the pseudonymity of blockchain. It is therefore necessary to define new approaches to effective law enforcement.

Other circumstances apply to closed systems. The enforcement of legal principles and standards is easier there. The appropriate *gatekeepers* are suitable regulatory addressees. Traditional approaches to regulatory law can be used without further ado in this extent.

The automation of contract management has been discussed since the mid-1990s under the heading of *smart contracts*. Contrary to the term itself, smart contracts are not contracts in the legal sense, but rather the linking of contracts with reality. Certain features of blockchain technology can now prove to be very useful in automating this performance:

- The decentralized validation of transactions allows for automated contract execution on a peer-to-peer basis.
- Blockchain technology makes it possible to embed values in the form of tokens directly into a contract, guaranteeing the contract execution without any credit risk.
- Blockchain technology can automate the execution of contracts so that subsequent unilateral changes to the process are no longer possible.

Blockchain is credited with the potential to dramatically lower transaction costs, particularly through the elimination of intermediaries. This creates potential for new contracts and types of contracts that would have been unviable to date, especially in the context of *micro payments*. In all of this, however, it is important to note that the automation of law has (and must have) limits. Value decisions cannot be replaced by technology, and it is important that property rights are not circumvented. State jurisdiction has to remain accessible and essentially effective.

In addition to individual contractual relationships, some relationships in the field of corporate law can also be settled on the basis of blockchain. So-called *decentralized* autonomous organizations (DAOs) are based on this idea. Tokens are used as voting rights within the "company." Innovative organizational forms and financing fundamentals can be economically stimulating. However, the resulting issues in terms of society and the law of obligations are still largely unexplained.

For data protection, blockchain offers opportunities just as it does challenges. This becomes particularly clear in consideration of open systems: on the one hand, the database and the trust in it are based precisely on the transparency of all the transactions. On the other hand, the technology is based on the use of pseudonyms and, in particular, therefore ultimately incorporates the idea of privacy-by-design. Conflicts between the blockchain approach and general data protection regulation may particularly arise with regard to accountability for data processing and the right to be "forgotten."

In order to foster innovation, it is possible to define navigating sandboxes, although the general regulatory framework necessary for such a purpose would create market access barriers which would be too high, without incurring irresponsible dangers. It is therefore important to ensure that appropriate due diligence measures are applied when predefined thresholds are exceeded.

In the medium term, however, a regulative laisser faire approach will not be enough. Changes to the legal system will be necessary, both to prevent dangers as well as to enable further innovation. On the one hand, the potentially rapid growth of individual applications may result in new systemic challenges, including for the legal system. The freedom required for the development of the technology therefore has to be accompanied by investments in monitoring and the development of stress tests. This also particularly applies in connection with smart contracts. On the other hand, adjustments to the regulatory framework are needed in order to make innovation possible. One obvious example concerns formal requirements: blockchain has potential in the area of transaction verification. However, the law is not exactly technologically neutral in this respect. The potential is therefore contingent upon the recognition of the technology as a suitable form of the respective business. Regulatory restraint is not enough to promote innovation in this respect.

3.10 Darknet

In terms of the social conflict of interests, darknet as the field of application of blockchain and of the cryptocurrencies it enables stands between the free and unobserved exchange of information and goods and the interests of law enforcement.

In addition to the indexed WWW, which is easily accessible by the public as well as by Google and other search engines, other forms of the Internet are known of today. Some of these are specifically designed to facilitate communication, data exchange and trading that are difficult or impossible to understand. They are often summarized today under the term *darknet*. These are channels on the Internet that are also used for illegal purposes. These include marketplaces such as *Silk Road* and numerous forums in the *Tor network*, where connection data is anonymized, as well as exchange platforms for software and media.

The darknet has gained in relevance, since it offers a seemingly law-free space which is not immediately accessible from the rest of the Internet, which provides space for extremist messages, criminal ideas and criminal trafficking and which serves as a means of communication and interaction. As a result, the darknet has created an environment that is very attractive to radicals and criminals, due to the promise of anonymity and non-traceability. It is important to not overlook the fact that there are, of course, numerous legal and traceable forms of use in the darknet which exclusively pursue the aspect of the free and unobserved exchange of information and which even offer protection from persecution in repressive and dictatorial systems.

Most cryptocurrencies in use today (such as bitcoin, hereafter used pars pro toto for cryptocurrency) use blockchains as a database. This blockchain is always visible to every trading partner. Entities between which bitcoins are transferred are so-called bitcoin wallets. They are not tied to the identity of a person per se and can be generated in any number, so that partners of a bitcoin transaction can usually remain anonymous. Accordingly, bitcoin is also used as the currency for conducting illegal trades in the darknet, such as those involving drugs, weapons and child pornography.

Law enforcement agencies have an interest in detecting illegal acts in the darknet. The respective aim is to find out to what extent the legally compliant observation of bitcoin transactions of known trading partners (e. g., known wallets, possibly associated identities) and the legally compliant collection of additional data on trading venues in the darknet (e. g., offered goods, assignments of nicknames to wallets) permit further conclusions regarding the nature of the transaction, the traded commodity as well as additional information about the identities of the respective trading partners.

3.11 Criteria for using blockchain

The different fields of application described in this section show that the use of a blockchain solution under certain conditions has great potential. In this regard, processes that are subject to strict regulation should not be selected.

In summary, this is the case if one or more of the following criteria are met.

1. **Intermediaries:** In the application in question, intermediaries can or should be bypassed in the process. Companies should therefore look at their processes and business models to see if they themselves can either act as intermediaries or optimize processes that require an intermediary. The use of a blockchain is useful when the intermediary

   a. incurs costs for the process steps when such costs can also be provided by functions of the blockchain

   b. delays a process and a blockchain application can speed it up

   c. there are political reasons for switching from a centralized intermediary-led process management to a decentralized one

2. **Data and process integrity:** For the application, a retroactive immutability of the transactions as well as a precisely specified execution are necessary.

3. **Decentralized network:** The use of a network for validating or passively using nodes that perform processes autonomously is reasonable and/or possible. This is relevant for all processes involving flexible, new and volatile cooperation partners without a stable and secure basis for transactions and trust. In such a case, a blockchain can guarantee networked integrity.

4. **Transmission of values and maintenance of rights:** blockchains enable the transmission of values and rights. Therefore, all processes in which originals, guarantees of origin or rights have to be transported or transferred are relevant.

4
CONTRIBUTIONS AND EXPERTISE WITHIN THE FRAUNHOFER-GESELLSCHAFT

4.1
Blockchain Laboratory – conception, development and evaluation

The various dimensions of the concept of a blockchain require a multidisciplinary approach to unlock the potential of distributed transaction management with its innovative approaches to consensus building. The Blockchain Laboratory of the **Fraunhofer Institute for Applied Information Technology FIT** addresses this aspect as an experience lab for technological components, implementation platforms, prototypical applications as well as blueprints for innovative governance and business models. It is a multidisciplinary institution for the conception, development and evaluation of blockchain solutions and has its roots in three research areas of the institute:

- Computer-aided group work for consensus finding
- Blockchain use case and business model development, prototypical blockchain applications
- Legal aspects (in cooperation with the *University of Münster*)

The aim of the laboratory is to demonstrate the current scientific findings in the still recent field of research with practicable, integrative applications.

In doing so, great value is placed on short development cycles in order to work quickly and in close cooperation with the partner companies in developing functioning applications which are then successively converted into marketable solutions. The development of these individual and needs-based solutions takes place in one-day or multi-day workshops, in applied research projects (from the potential analysis to implementation) as well as in industry-wide and cross-industry consortia.

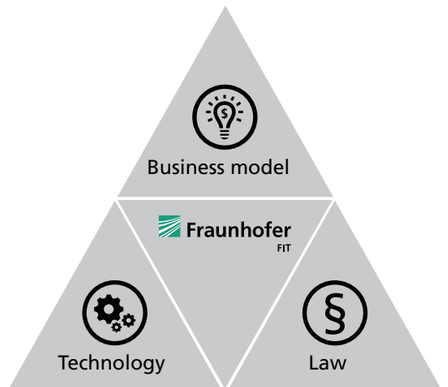

Fig. 4: The multidisciplinary approach of the Blockchain Laboratory

As Figure 4 illustrates, the integrative solution offerings are based on the triad of business model, technology and law. Business model development is customer- and industry-specific and includes the potential analysis, classification and development of

disruptive solutions. The focus of the technology implementation is the provision of a development platform with different blockchain systems (P2P network, validation server, etc.), the implementation of blockchain solutions and the evaluation of blockchain concepts. The legal consideration includes advice concerning the legal aspects to be considered as well as the evaluation of blockchain systems and business models, taking into account valid regulatory requirements.

The results of the activities of the blockchain laboratory are individual solutions in complex application areas based on blockchain concepts: smart contracts and decentralized autonomous organization for more efficient governance and processes. Areas of application include (among other) the Internet of things, (intellectual) property management, stock market trading, asset management and clearing processes.

4.2
Blockchain Security Laboratory – security

The Blockchain Security Laboratory is designed to accumulate expertise, investigate attacks, and develop security technologies for blockchain-based applications.

In practice, there is not a single blockchain technology; instead, entire stacks are assembled from multiple technology blocks, on the basis of which blockchain applications can be implemented and executed. These stacks include the actual peer software, peer-to-peer overlay protocols, consensus protocols, blockchain APIs, and the actual applications. The large number of variants of permissioned/permissionless ledgers with different mining strategies or trust models results in an entire landscape of blockchain-based applications, each of which have different characteristics.

In order to evaluate their behavior in different borderline situations or to validate their correctness, the Blockchain Security Laboratory of the **Fraunhofer Institute for Applied and Integrated Security AISEC** can set up appropriate infrastructures of realistic size and perform typical attacks. These include, among others:

- Over 50% attacks on blockchains with proof-of-work-based consensus protocols, whereby an attacker with sufficient resources can himself produce consensus and thereby modify blockchain content
- Other structural majority attacks, such as selfish mining, in which a group of attackers initially withhold their find and already begin to calculate the next block without the knowledge of other miners, with the goal of gaining a temporal advantage and a higher profit or to manipulate transactions
- Known attacks on P2P networks, such as the targeted manipulation of individual nodes and creating the misconduct of the majority of the validating peers
- Investigation of failures in smart contract implementations or the associated execution environments
- Validating the correctness of smart contract implementations

The primary goal of the Blockchain Security Laboratory is to develop expertise regarding blockchain security which can be used, on one hand, in services and, on the other, as a foundation for developing security technologies for currently unresolved blockchain technology issues. The Blockchain Security Laboratory therefore includes three components:

- Building a technical infrastructure and testing known attacks
- Developing secure smart contracts, applying formal verification methods to smart contracts
- Developing a training offering for industrial customers

4.3
Cyber security consulting

The **Fraunhofer Institute for Secure Information Technology SIT** supports companies and institutions in designing and evaluating blockchain and smart contract concepts, projects and systems with regard to IT security and privacy. Both blockchain technology as well as the smart contracts that are built upon it have promising characteristics of security, trustworthiness and privacy with the added prospect of increasing efficiency for many applications. The distributed-ledger technology with its security features could also be the signalman for digital innovations and the associated new business models.

A safety analysis by the Fraunhofer SIT will provide important information early on (for example, already during the idea and conception phase) concerning the accessibility of protection goals of IT security and the effectiveness of measures for privacy protection. To improve the security of software, IT services and IT systems, it is imperative that security and privacy be considered from the outset and then considered over the complete life cycle. The subsequent correction of decisions regarding the protection goals to be achieved, the security mechanisms chosen for this purpose and the subsequent protection of weak points are usually difficult and expensive. The Fraunhofer SIT supports companies and institutions in implementing the two paradigms of *security-and-privacy-by-design* and s*ecurity-at-large*.

The security of blockchain systems should be distinguished from the security of blockchain applications. If a particular wallet software has serious security vulnerabilities, for example, then it does not provide any assurance about the security properties and the merit of the implementation of the underlying blockchain system.

The following topics are the focus concerning the **security of blockchain systems**:

Consensus algorithms

Under certain conditions, several equal parties (the so-called peers) in a communication network can bring about a common agreement [10]. If the agreement is decentralized, it will be accompanied by a higher fault tolerance and a stronger trust model than is offered by central approaches. In a central approach, such as with only one central location, this location typically represents the bottleneck in terms of trust and availability. In a decentralized case, agreements can be reached even if the parties include participants that are not communicating (e. g., because they are offline) [12] or otherwise do not contribute towards agreement, e. g., because they are flawed or corrupt. Corrupt in this regard means that these parties are trying to maliciously counteract or manipulate the agreement – typically out of unfair self-interest [14].

The bitcoin blockchain is permissionless and public, and any actors worldwide can join it. The bitcoin blockchain includes a proof-of-work procedure that allows fair agreements to be reached even if it is not currently know which actors are uncooperative in what ways. For this purpose, however, certain conditions have to be met during operation, such as that a certain ratio of computing capacity of uncooperative parties

to cooperative parties is not exceeded. Incentivizing the miners in the proof-of-work processes should also ensure that a network-based attack and selfish mining become more expensive than compliant mining. There is a trade-off in terms of efficiency and security in this regard, though: the higher the value of a transaction, the longer it is necessary to wait until the transaction can be considered to be registered reliably.

For distributed agreements, there are a number of algorithms to choose from, such as Byzantine algorithms, proof-of-X procedures and combination algorithms. These are suitable for different requirements, such as functionality (current altitude in the case of conflicting data from independent altimeters in an airplane), efficiency (real-time requirements), compliance (bank review requirements), privacy protection (personal data) and security (assumed attacker model). In addition, the security requirements of permissioned blockchains are very different from those of permissionless blockchains.

A security analysis by the Fraunhofer SIT supports the decision for the consensus algorithm to be selected for blockchains.

Transparency of all transactions

In addition to the disclosure of information, safety and privacy considerations also have to be considered. Even in a private blockchain, all the authorized actors are aware of the complete accounting system of the blockchain; in a public blockchain, this potentially applies to the whole world. This transparency can result in both a gain as well as a loss of security and/or privacy, depending on the considered protection goals and purpose of the blockchain (particularly concerning the spectrum of applications that it is intended to be able to use).

Code = Code?

The Dogma (program) code = (legal) code, i.e., the programming code establishes the rules for a blockchain or smart contracts even for conflict cases and can no longer be corrected; this has to be considered critically: It is unlikely that programs above a certain number of lines do not contain any errors. Therefore, it is highly recommended that regulations (especially for the potential "failure" of program codes, in terms of both functionality as well as IT security) be agreed upon and announced as soon as upon the launch of blockchains and smart contracts, and that they and their limitations be designed with the program code such that they can be changed agilely over the entire life cycle. The question of what it means when a minority does not want to abide by the decisions of the majority is very relevant (see, for example, previous *hard-forks*).

Cryptography

The cryptographic procedures used in a blockchain system have to be evaluated with regard to their current security level (including potential implementation weaknesses), their ease of change and their likely future viability.

"Classic" attack vectors

Of course, the implementation of a blockchain also has to be protected, according to its underlying attacker model, against attacks that are not specific to blockchains. In addition to the security of blockchain as a technology, the safety of the applications that it makes possible also has to be considered. Prominent examples from the field of cryptocurrencies are attacks on wallets (where are the private keys stored: *hot storage* vs. *cold storage*?) and attacks on exchange platforms (e. g., Mt Gox, Cryptsy, Bitfinex hack).

4.4 Forensic consulting

The proactive forensic consulting of the **Fraunhofer Institute for Secure Information Technology SIT** follows the principle of *forensic readiness* – this of course also applies to blockchain applications. Reactive forensics consulting in the blockchain context is primarily targeted towards law enforcement agencies.

Forensic readiness refers to the preparation for the IT forensic investigation of incidents, enabling an effective and efficient response to future attacks. Forensic readiness is especially important for a relatively young technology, such as blockchain, that has potentially unknown attack vectors which are very different depending on the application. In messages concerning incidents and attacks, it is repeatedly read that the persons concerned "did not expect it" and appropriate mechanisms which would facilitate being informed in that regard or even make it possible were not applied. Although many future attacks cannot be foreseen in concrete terms, the damage potential – even of previously unknown attacks – can still essentially be estimated and categorized. Technical and non-technical measures such as insurances or alternative risk transfer can be effective in such a context. In this regard, the Fraunhofer SIT offers its many years of experience in IT forensics for effective and efficient prevention and risk assessment –particularly concerning companies that have a business models based on blockchain technology and users of mission-critical information technology (e. g., banks, insurance companies, energy suppliers) that intend to begin using this technology.

Another focus is on law enforcement agencies: based on the number and severity of the incidents, law enforcement agencies are interested in forensics for blockchain systems in cryptocurrencies and, specifically, in the related investigation of crimes, such as ransomware extortion or illegal trading in darknet. While the pseudonymity of cryptocurrency transactions complicates investigations, authorities have at their disposal a large portfolio of state-of-the-art IT forensic methods and research to detect illegal acts. The respective methods have to be categorized, further developed and evaluated with regard to their effectiveness.

The Fraunhofer SIT is available to the authorities in this regard as a proven partner for intelligence which is in compliance with fundamental rights and the law. In the investigation of crimes, it can make blockchain data tracks in the darknet accessible and can analyze them. Even if the perpetrators use forensic defense mechanisms, investigators can often obtain the data they need. In such a procedure, particular care always has to be taken to ensure that the evidential value of the data is preserved.

4.5 Cost-effectiveness

Surely, one of the central questions with regard to the implementation of blockchains is the question of their profitability. A sweeping answer to this question is not possible. A conceptual-architectural consideration of blockchain technology basically leaves the question open as to whether a public blockchain can even function permanently under economic aspects. The bitcoin blockchain, for example, requires a lot of energy to maintain the system, due to the communication-intensive process and the computationally intensive mining. Another negative aspect is the redundant data storage, which requires a lot of storage capacity, which can also lead to considerable costs. In addition, in public projects for transactions (data storage), low fees generally apply which, as a result of scaling effects, are not insignificant.

It depends upon the public nature (public/private) of the blockchain and the specific application, among other things. Basically, it should be noted that many of the private blockchain solutions are open source projects and are therefore not linked to complex licensing models. In addition, administrations can reduce time-consuming proofing procedures. The complexity of today's value chains and networks also requires a multi-dimensional approach. The **Fraunhofer Institute for Material Flow and Logistics IML** is developing a demonstrator-based solution that can simulate and calculate an end-to-end view along the supply chain for the specific application. Fraunhofer uses different methods to evaluate non-public systems in supply chain management and purchasing.

Another challenge of the economic evaluation is the quantification of trust. As already described, blockchain represents a technology that can resolve the issue of trust that is currently ensured in various industries through third-party fee-based services (payment service providers, credit card companies).

It should therefore be noted that a statement regarding a business case can only be made in consideration of the specific application. The already mentioned efforts that arise during the implementation and operation of the blockchain technology, as well as the direct monetary benefits which are due, for example, to process optimization (among other reasons, through effort reduction, acceleration of manual processes) form the basis for a comprehensive business case evaluation.

However, since the predictions of monetary dimensions in a certain forecast period are highly uncertain, it makes sense to use not only the pure monetary valuation but also the (indirect) qualitative potential benefits for a holistic view of a business case. These could include: an increase in company value through horizontal networking with value-added partners, a reduction in the complexity of administrative processes, safer transaction processing, protection against manipulation, closer orientation to regulatory requirements, etc.

Extended to include potential risks (including the current state of technology, consequences of a system failure, hacker attacks, etc.), the use of an example of blockchain technology can therefore be assessed comprehensively.

For this purpose, the Fraunhofer IML has developed the **Blockchain Business Case Calculator** in the institute's own laboratory and in dialogue with industrial partners. The development is intended to enable a multi-dimensional and interdisciplinary analysis of the economic viability of the use of blockchain technology along the value chain, thereby making an essential contribution to securing the investment decision in the company.

4.6
Technology foresight

The **Fraunhofer Institute for Technological Trend Analysis INT** offers scientifically-based assessment and consulting expertise across the entire spectrum of technological developments. On this basis, the institute conducts technology foresight, making possible a long-term approach to strategic research planning. This enables the conception of an overall perspective on future technologies in regard to their whole dynamics and complexity. Future applications and possible implementations of the analyzed technologies in the field of blockchain resp. *distributed ledgers* can thus be assessed in a comprehensive and scientifically-sound manner so that an early utilization of related potentials will be possible and challenges can be overcome. In this case, the interrelations with robotics, miniaturization, the Internet of things, cloud and edge computing, big data, VR/AR, cyber security and artificial intelligence, among others are to be factored in.

By applying a variety of different methods of future studies like various quantitative techniques as well as qualitative meta- or in-depth-analyses, road mapping, scenario techniques or serious games, "present futures" (that means the futures we imagine today) can be investigated[11]. In addition to the technological aspects, especially societal, political, economic, legal and regulatory issues can determine whether this technology will develop into a disruptive innovation, given the conflicting areas between security, trust, responsibility and functionality, or whether it will merely be reduced to a supplementary product.

Current concepts and implementations address the scalability and performance issues of the bitcoin blockchain and/or cover a wide variety of privacy issues. Other challenges include the heterogeneity of the various types of implementation technologies, business models and use cases, the influence of new emerging power and dependence structures (such as mining pools) as well as new intermediaries (re-intermediation). With the connectivity to the real world, difficulties arise in ensuring comprehensive security. Additional issues include the lack of interoperability and standardization, norms and governance structures, regulation and legislation, as well as infrastructure issues.

The Fraunhofer INT can support business, politics and civil society with a competent assessment of research and action requirements in the field of blockchain and distributed ledgers and can also develop alternative (technological) problem-solving concepts.

4.7
Industrial Data Space IDS

The **Industrial Data Space Initiative**[12] is aimed at creating an international standard for data sovereignty. Data sovereignty is the ability of a natural or legal person to exclusively self-determine his/its data assets. This capability is a key requirement for businesses in the digital economy, since all smart service scenarios, as well as many innovative, digital business models, rely on data owners/possessors being able to exchange their data in business ecosystems, while at the same time not having control over that data.

The Industrial Data Space Initiative is currently institutionalized as a research project and user association. In the research project, the Fraunhofer-Gesellschaft designs the reference architecture model and pilots it in various fields of application. The project works closely with the user association, which bundles the interests of the industry, introduces requirements and is responsible for the standardization. The reference architecture model enables information technology support of data sovereignty. It is based on design principles that guide the execution of specific implementations. These include, among others:

11 The support for identifying development options for politics, civil society and the economy can be optimized by collaborating with other institutes of the Fraunhofer-Gesellschaft that either focus on innovation systems and bring in complementary competencies to the Fraunhofer INT, or are dedicated to specific technologies.

12 see http://www.industrialdataspace.org/

- **Decentralized data storage:** The industrial data space is a decentralized data space without compulsory central data storage, such as those found in the IoT cloud solutions or *data lakes*.

- **Terms of use:** Data owners and possessors also have to be able to contribute their own terms of data use before they are exchanged. In the sense of so-called *sticky policies*, the data therefore has to contain information about the circumstances under which it may be read or used and by whom.

- **Protection of trust:** All participants have to be trustworthy, i.e., both software that grants access to the industrial data space as well as companies that operate such software have to be certified. The certification criteria are defined by the user association.

- **Business ecosystem:** The industrial data space manifests itself as the virtual space of endpoints. The endpoints form various roles, such as data providers, data users, brokers of the data supply and data demand, a clearing house as well as providers of *data apps* and *identity services*.

The industrial data space is therefore a decentralized architectural design for promoting data sovereignty in the digital economy. In this context, data is a separate asset that is exchanged in business ecosystems, has value and for the exchange of which cash flows are generated. Payments are based on data transactions between data providers and data users or multilaterally in the data network. In order to be able to process payments for data, it is necessary to record and store the corresponding data transactions.

In the sense of the decentralized architectural paradigm of the industrial data space, blockchain technology as a concept for the decentralization of payment transactions basically represents a variant for the implementation of data transaction management which is in the industrial data space within the responsibility of the clearing house. The use of blockchain technology in the industrial data space is also very promising due to the fact that, in particular, requirements for data provenance and data traceability in data networks can be covered by the blockchain properties. The Industrial Data Space Initiative is currently evaluating the use of blockchains in various data-network use cases.

5
GLOSSARY

Altchain: Alt(ernative) chains are proprietary blockchains or distributed ledgers which are usually associated with independent cryptocurrency. There are currently 788 cryptocurrencies with a total market capitalization of USD 70 billion (as of July 2017). These include Ethereum, Ripple, Litecoin, Ethereum Classic, NEM, Dash, IOTA, Bitshares and Monero, just to name a few.

BitTorrent: is a collaborative file-sharing protocol that is particularly well suited for the rapid distribution of large volumes of data.

Decentral autonomous organization (DAO): A DAO is a blockchain-based, autonomous, decentralized organizational unit that makes its own decisions based on an algorithm.

Distributed ledger: A distributed ledger is a public, decentralized journal that normally chronicles all transactions of a business.

Fintech: An acronym for financial technology, a term for new financial services that rely on Internet technologies, including blockchains.

Hard fork: An irreversible division of a blockchain into two incompatible continuations.

Hash function/hash value/hash tree: Mapping methods used to generate new blocks of a blockchain to make the blocks tamper-proof.

Intermediary: A transaction facilitator that guarantees the correctness of the process and whom the involved partners trust.

IT forensics: *IT forensics* deal with the investigation of suspicious incidents in connection with IT systems as well as the determination of facts and perpetrators by recording, analyzing and evaluating digital traces.

Cryptoagility: The ability in an encrypting system to replace cryptographic procedures that have become unsafe with new, widely secure ones.

Cryptocurrencies: A virtual, digital currency that uses blockchains as a transactional protocol and employs cryptographic techniques to protect against tampering.

Micro-payment: Transactions of very small amounts of money that were not worthwhile in the past because the transaction costs exceeded the value of the amount.

Nonce: (short for: *used only once* or *number used once*) In cryptography, the term nonce is used to denote a combination of numbers or letters used only once in the respective context.

Payment channel networks: Payment channel networks are concepts for a network for payment transactions that is parallel to the blockchain, does not require any transaction fees and enables maximum confidentiality. They are currently in the experimental implementation phase.

Prosumer: An abbreviation for persons or companies that are both producer and consumer.

Pruning: A way to remove unnecessary data about transactions that have been fully executed.

Pseudonymity: The executors of transactions are unknown, but under certain circumstances ascertainable.

Sharding: Individual computers "administrate" only different partitions of the blockchain locally.

Sidechains: Sidechains use bitcoins as seed to build their own blockchain based thereupon.

Smart contracts: Computer-based contracts that are automatically executed according to certain rules and are logged in blockchains, for example.

Smart oracle: The term smart oracle becomes established when it comes to incorporating a real-world status into a smart contract.

Distributed consensus building: A process that determines the validity of a transaction through a distributed evaluation process.

Zero knowledge evidence: Protocols whereby one party persuades another to know a secret without revealing it.

6
LITERATURE

1 Abadi, Martin, Burrows, Mike, Manasse, Mark, and Wobber, Ted, "Moderately Hard, Memory-bound Functions," ACM Trans. Internet Technol. 5, no. 2 (2005): 299–327, https://doi.org/10.1145/1064340.1064341.

2 Back, Adam. Hashcash – A Denial of Service Counter-Measure, 2002, http://www.hashcash.org/papers/hashcash.pdf.

3 Baran, P., "On Distributed Communications Networks," IEEE Transactions on Communications Systems 12, no. 1 (1964): 1–9, https://doi.org/10.1109/TCOM.1964.1088883.

4 Daswani, Neil, Garcia-Molina, Hector, and Yang, Beverly, "Open Problems in Data-Sharing Peer-to-Peer Systems," Database Theory — ICDT 2003 (2003): 1–15, https://doi.org/10.1007/3-540-36285-1_1.

5 Dwork, Cynthia, and Naor, Moni, "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology," CRYPTO'92: Lecture Notes in Computer Science (1993), 139–147, Retrieved from http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.ps.

6 Gideon, Gottfried, "Aus für die Global Repertoire Database: PRS will Alternative," MUSIKMARKT (2014), http://www.musikmarkt.de/Aktuell/News/Aus-fuer-die-Global-Repertoire-Database-PRS-will-Alternative.

7 Giechaskiel, Ilias, Cremers, Cas, and Rasmussen, Kasper Bonne, "On Bitcoin Security in the Presence of Broken Crypto Primitives," IACR Cryptology ePrint Archive (2016): 167, http://ai2-s2-pdfs.s3.amazonaws.com/2377/2e1eb97b39865aee0a3b3e83b0d87d0798ab.pdf.

8 Hammer, Michael, and Champy. James, Reengineering the Corporation: A Manifesto for Business Revolution (Harper Business, 1993).

9 Hanson, R.T., Reeson, A., and Staples, M., Distributed Ledgers, Scenarios for the Australian economy over the coming decades (2017). Retrieved from Canberra.

10 Jameson, Hudson, Hard Fork No. 4: Spurious Dragon – Ethereum Blog. March 16, 2017. https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/.

11 King, Sunny, and Nadal, Scott, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August 19. March 19, 2017. http://peerco.in/assets/paper/peercoin-paper.pdf.

12 Lamport, Leslie, Shostak, Robert, and Pease, Marshall, "The Byzantine Generals Problem," ACM Trans. Program. Lang. Syst. 4, no. 3 (1982): 382–401, https://doi.org/10.1145/357172.357176.

13 Ongaro, Diego, and Ousterhout, John, "In Search of an Understandable Consensus Algorithm," Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference (USENIX ATC'14, 2014), 305–320, Retrieved March 16, 2017 from http://dl.acm.org/citation.cfm?id=2643634.2643666.

14 Pease, M., Shostak, R., and Lamport, L, "Reaching Agreement in the Presence of Faults," J. ACM 27, no. 2 (1980): 228–234, https://doi.org/10.1145/322186.322188.

15 Pouwelse, Johan, Garbacki, Pawe\l, Epema, Dick, and Sips, Henk, "The bittorrent p2p file-sharing system: Measurements and analysis," International Workshop on Peer-to-Peer Systems (2005) 205–216, Retrieved March 16, 2017 from http://link.springer.com/10.1007/11558989_19.

16 Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," March 16, 2017. https://bitcoin.org/bitcoin.pdf.

17 Tapscott, Don, and Tapscott, Alex. Die Blockchain-Revolution: Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert (Plassen Verlag, 2016).

18 UK Government Office for Science. Distributed Ledger Technology: beyond block chain, June 27, 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

19 Schlatt, Vincent, Schweizer, André, Urbach, Nils, and Fridgen, Gilbert. Blockchain White Paper: Grundlagen, Anwendungen und Potentiale. Fraunhofer FIT 2016 https://www.fit.fraunhofer.de/blockchain.

20 Znati, Taieb, and Abliz. Mehmud, "A Guided Tour Puzzle for Denial of Service Prevention." Computer Security Applications Conference, Annual (2009), 279–288, https://doi.org/10.1109/ACSAC.2009.33

21 Whitepaper:Nxt. https://nxtwiki.org/wiki/ :Nxt.