Attacking the trust machine

Developing an information systems research agenda for blockchain cybersecurity

Schlatt, Vincent; Guggenberger, Tobias; Schmid, Jonathan; Urbach, Nils

DOI
10.1016/j.ijinfomgt.2022.102470

Publication date
2023

Document Version
Final published version

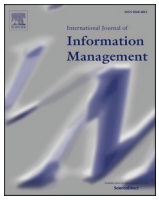
Published in
International Journal of Information Management

International Journal of Information Management 68 (2023) 102470

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



Review Article

Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity

Vincent Schlatt [a,b,c,*], Tobias Guggenberger [a,b,c], Jonathan Schmid [d], Nils Urbach [a,b,e]

[a] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Bayreuth, Germany
[b] FIM Research Center, Germany
[c] University of Bayreuth, Bayreuth, Germany
[d] Delft University of Technology, Delft, The Netherlands
[e] Frankfurt University of Applied Sciences, Frankfurt am Main, Germany

ARTICLE INFO

Keywords:
Blockchain
IT Security
Structured literature review
Research agenda

ABSTRACT

Blockchain-based systems become increasingly attractive targets for cybercrime due to the rising amount of value transacted in respective systems. However, a comprehensive overview of existing attack vectors and a directive discussion of resulting research opportunities are missing. Employing a structured literature review, we extract and analyze 87 relevant attacks on blockchain-based systems and assign them to common attack vectors. We subsequently derive a research framework and agenda for information systems research on the cybersecurity of blockchain-based systems. We structure our framework along the users, developers, and attackers of both blockchain applications and blockchain infrastructure, highlighting the reciprocal relationships between these entities. Our results show that especially socio-technical aspects of blockchain cybersecurity are underrepresented in research and require further attention.

1. Introduction

Blockchain-based systems become increasingly relevant in business and society. While the blockchain technology originally gained traction as the backbone of the digital currency Bitcoin, a multitude of applications ranging from supply chain management (Bumblauskas, Mann, Dugan, & Rittmer, 2020; Guggenberger, Schweizer, & Urbach, 2020; Liu & Li, 2020), financial services (Ali et al., 2020) to the Internet of Things (Chanson, Bogner, Bilgeri, Fleisch, & Wortmann, 2019; Lockl, Schlatt, Schweizer, Urbach, & Harth, 2020) exists today. These applications aim at leveraging the inherent characteristics of the technology, such as decentralization, tamper-resistance, and transparency (Hughes et al., 2019; Schweizer, Schlatt, Urbach, & Fridgen, 2017).

As a result, blockchain-based systems hold an increasing amount of value, both monetary and in the form of business process information. For example, the total value of all Bitcoins in circulation is valued at USD 795 billion as of January 2022 (CoinMarketCap, 2022). Moreover, many blockchains facilitate smart contracts, allowing individuals and organizations to implement arbitrary business logic on a decentralized infrastructure. Consequently, such systems can maintain crucial information for business processes. For example, the German Federal Office for Migration and Refugees develops a blockchain-based system for managing highly sensible refugee identities along the asylum process (Guggenmoos, Lockl, Rieger, Wenninger, & Fridgen, 2020), while a consortium of shipping companies processes global container shipping flows through blockchain technology (Jensen, Hedman, & Henningsson, 2019).

This ever-rising value stored in blockchain systems creates increasingly attractive targets for attackers. Recent years reported several prominent cybercrimes on respective systems. In addition, blockchain-based systems have become increasingly complex. The DAO, supposedly the first completely decentralized organization based on blockchain, became the victim of a famous hack in 2016, leading to a loss of USD 50 million for its investors at the time (Mehar et al., 2019). In the realm of cryptocurrencies, the currency exchange Mt. Gox suffered several attacks resulting in the decay of the exchange with severe consequences for its customers (Feder, Gandal, Hamrick, & Moore, 2017).

Despite the relevance of such incidents, the cybersecurity of blockchain-based systems has been considered as being strong by information systems (IS) research so far (Frizzo-Barker et al., 2020; Hughes et al., 2019). However, several researchers called for a more critical perspective (Beck, Avital, Rossi, & Thatcher, 2017; Hughes et al.,

* Corresponding author.
E-mail address: vincent.schlatt@fit.fraunhofer.de (V. Schlatt).

https://doi.org/10.1016/j.ijinfomgt.2022.102470
Received 29 December 2020; Received in revised form 9 January 2022; Accepted 10 January 2022
Available online 21 January 2022

2019) and additional research on the security of blockchain (Mendling et al., 2018). While initial technical surveys on the security of blockchain-based systems exist, the IS community lacks a systematic overview of attack vectors and resulting research avenues. However, research on the security of blockchain technology is required to increase acceptance of (Saad et al., 2020) and trust in its applications (Hughes et al., 2019). In summary, while the security of blockchain-based systems seems "virtually indisputable" in IS literature, it is nevertheless considered a risk (Frizzo-Barker et al., 2020, p. 9). IS researchers and practitioners alike should holistically consider the cybersecurity threats to blockchain-based systems to design, develop, and evaluate applications based on such systems (Warkentin & Orgeron, 2020). To fill this research gap, we aim to answer the following question:

> *What are known attack vectors of blockchain systems and which IS research avenues concerning the cybersecurity of blockchain-based systems can be derived?*

We answer this question by collecting and analyzing attacks on blockchain-based systems through a structured literature review (SLR). As such, we cover both public and private as well as permissioned and permissionless blockchains. We identify a total of 87 relevant attacks and subsequently structure them along a generic blockchain technology stack. Based on the findings of the SLR, we derive a comprehensive research framework and agenda for the interdisciplinary IS community. Thus, we aim at contributing to the discussion on the attack vectors and security threats to blockchain-based systems and proposing a comprehensive collection of resulting future research opportunities. As a result, this article aids practitioners in building secure applications by providing an overview and context of existing attacks on blockchain-based systems.

The remainder of this paper is structured as follows. Section 2 sets the necessary foundations, covering blockchain and related cybersecurity research. Section 3 describes the research method, while Section 4 presents and discusses the attack vectors identified in the SLR. Section 5 derives a comprehensive IS research framework and agenda for blockchain cybersecurity from the analysis of the previously identified attacks. The following Section 6 provides an extensive discussion of this paper's contribution and implications, while Section 7 closes the paper with a conclusion.

2. Foundations

2.1. Blockchain technology

Blockchain is a novel type of a highly resilient distributed data structure, which allows redundantly storing transactions grouped in blocks on the nodes of a peer-to-peer (P2P) network (Glaser, 2017). Each block is linked with its predecessor by referencing the hash value of the previous block. To issue a new transaction, a client propagates it to the blockchain network. Peers collect these transactions, group them in a block, and propose this block according to specified rules to the network. A consensus mechanism then ensures that the system's peers agree on a common state of the blockchain. Once an agreement is reached on a block, the respective peers append it to their blockchain (Chanson et al., 2019).

To increase the applicability of blockchain-based systems, different concepts of blockchain arose over the past decade. A popular categorization by Peters & Panayi (2015) distinguishes between public blockchains, where transactions are publicly visible, and private blockchains, where transactions are only visible to authorized parties. Furthermore, permissionless blockchains allow anyone to participate in the P2P network and validate transactions, while Permissioned systems retain this right to authorized parties exclusively. Along these architectural dimensions, different consensus mechanism alternative to the computationally intensive and, thus, inefficient proof-of-work in Bitcoin emerged (Sedlmeir, Buhl, Fridgen, & Keller, 2020). While some approaches offer improved scalability or efficiency, they require an increased amount of trust in the nodes participating in a blockchain network. Thus, they are so far mainly practicable in permissioned blockchain settings, where nodes are known and trusted to a certain extent.

Advancements of the basic technological concept allow for implementing arbitrary logic on blockchain systems through smart contracts (Schweizer et al., 2017). Smart contracts are computer programs, which are stored on the peers of the P2P network. When functions in these programs are invoked through transactions, the network's peers execute their logic redundantly. The smart contracts are transparently auditable by the peers participating in the network. Advanced ideas on the use of respective smart contracts involve developing nexuses of smart contracts creating decentral autonomous organizations (DAOs) (Beck, Müller-Bloch, & King, 2018), such as the previously mentioned The DAO. Management and operational rules in DAOs are encoded in autonomously operating smart contracts, which are controlled by their shareholders, thus creating organizations without a central management (Wang et al., 2019b; Ziolkowski, Miscione, & Schwabe, 2020). Applications of blockchain technology are wide-ranging and present in almost all sectors of industry (Frizzo-Barker et al., 2020), for example in humanitarian supply chains (Dubey, Gunasekaran, Bryde, Dwivedi, & Papadopoulos, 2020) or improved crowd forecasting methods (Rupasinghe, Burstein, & Rudolph, 2019).

In recent years, several generic research agendas concerning blockchain technology have emerged. While some explicitly consider the cybersecurity of blockchain-based systems and the risk resulting from their application as a critical topic, the majority focus on other areas of IS research and disregard this aspect. In addition, cybersecurity is often regarded as an inherent feature of blockchain systems, rather than a threat. Risius & Spohrer (2017); Beck et al. (2017); Rossi, Mueller-Bloch, Thatcher, & Beck (2019) as well as Lindman, Tuunainen, & Rossi (2017) do not explicitly mention cybersecurity as an avenue for IS research. However, the authors emphasize the importance of interdisciplinarity in research on blockchain technology. This aspect should be considered for constructing an IS cybersecurity research agenda for blockchain. Frizzo-Barker et al. (2020) focus on developing a business-oriented research agenda but acknowledge that security is considered an inherent characteristic in common definitions of blockchain technology. Nevertheless, the authors indicate that the security of blockchain-based systems can be both benefit and risk. Hughes et al. (2019) identify security as a distinct theme in IS research, and mention the reliance on public key infrastructure as an implicit cybersecurity threat. The authors state that research on the security of blockchain-based systems is required to increase trust in the technology. Considering the application of blockchain to emerging countries, Schuetz & Venkatesh (2020) emphasize the detrimental impact of security weaknesses in blockchain-based systems used by citizens in developing economies, while Warkentin & Orgeron (2020) assess information security through blockchain in the public sector.

2.2. Cybersecurity aspects of blockchain technology

Information security generally aligns along the C-I-A triangle comprising the goals of confidentiality, integrity, and availability (Whitman & Mattord, 2011). Research lately extended these foundational goals of information security to include authenticity, accountability, auditability, trustworthiness, non-repudiation, and privacy (Berger, Bürger, & Röglinger, 2020). Cybersecurity is broadly defined as "[t]he approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space" (Schatz, Bashroush, & Wall, 2017, p. 66). Cybersecurity attacks represent intentional and unauthorized access to systems and thus pose a threat to information systems' security goals (Miede et al., 2010). Attackers aim

to reach an unauthorized target by carrying out several planned steps to achieve their ultimate goal (Howard & Longstaff, 1998). Along the way, attackers employ tools facilitating the exploitation of vulnerabilities in a system. The attackers' motivations are diverse and depend on the attack, the attacked application, which layer of the information system is attacked, and many more aspects (Howard & Longstaff, 1998).

Blockchain technology represents a combination of previously existing technologies, which characterize its properties and provides IT systems security with new semantics. Blockchain technology's key security characteristics include aspects such as integrity, immutability, decentralization, and pseudonymity (Schweizer et al., 2017). Nevertheless, its inherent properties also introduce specific challenges to cybersecurity. The distributed nature, extensive use of cryptography, and information transparency exacerbate issues in secure software engineering. Properties such as backward immutability further introduce new security challenges. Several prominent examples illustrate that attacks exploiting vulnerabilities specific to blockchain technology are feasible and become an increasing threat to applications based on the technology. Yet, the technology is regularly hailed as inherently secure and applications can be found in multiple highly critical areas of society, such as supply chains (Garg et al., 2021) or detection of counterfeit products (Modgil & Sonwaney, 2019). Trust in blockchain and its security is often one of the major arguments for the adoption of the technology (Pournader, Shi, Seuring, & Koh, 2020). Thus, research on the actual level of cybersecurity and potentially compromising attacks is highly relevant.

The computer science community took up the lack of coherent overviews of attack vectors of blockchain-based systems from a technical perspective. However, many publications are focused on specific instantiations of blockchain-based systems and thereby limited in their scope and generalizability. Furthermore, they lack the derivation of an interdisciplinary research agenda suitable for the realm of IS. Accordingly, Conti, Sandeep Kumar, Lal, & Ruj (2018) present threats to security and privacy in Bitcoin and its proof-of-work consensus mechanism. Chen, Pendleton, Njilla, & Xu (2020) present an overview of vulnerabilities and attacks on Ethereum smart contracts. The findings are thus limited to the Ethereum blockchain. A further approach to structuring attacks limited to Bitcoin is given by Zhu et al. (2020). The respective authors systematize attacks, concentrating on the target surface of data by assigning attacks to three clusters: data privacy attacks, data availability attacks, and data consistency attacks. A publication by Rahouti, Xiong, & Ghani (2018) provides a further account of attack vectors of the Bitcoin blockchain system and its consensus mechanism.

Recently, more generic overviews of attacks on blockchain systems emerged sporadically in the computer science literature (Averin & Averina, 2019; Li, Jiang, Chen, Luo, & Wen, 2020; Morganti, Schiavone, & Bondavalli, 2018; Shrivas, Dean, & Brunda, 2020). While aiming to provide a comprehensive overview, the respective papers are still limited in their scope. Saad et al. (2020) provide an overview of attacks on blockchain technology by assigning 17 distinct attacks to three pre-determined attack surfaces related to blockchain system components. Based on these findings, the authors derive research avenues concerning the improvement of technical components of blockchain technology. Similarly, Homoliak, Venugopalan, Hum, & Szalachowski (2019) survey the security of blockchain-based systems. Furthermore, the authors define a reference architecture detailing weaknesses and potential points of attack. In sum, the authors identify 29 attacks but lack to derive avenues for interdisciplinary research from their findings. The paper identifying the largest amount of attacks presents 49 attacks (Shrivas et al., 2020) but misses to comprehensively derive future research opportunities. Also, the methodical approach of the respective papers often seems untransparent and, therefore, lacks reproducibility. For example, while Li et al. (2020) offer a systematic review of attacks on blockchain systems, they do not further describe how they gathered their data (i.e., stating search strings or databases). Magazzeni, McBurney, & Nash (2017) develop a research agenda limited to the verification and validation of smart contracts. Taylor, Dargahi, Dehghantanha, Parizi, & Choo (2020) offer a comprehensive literature review and research agenda concerning the security benefits gained from utilizing blockchain technology, but miss to shed light on the opposite effect, i.e., the security risk arising from blockchain.

3. Research method

Our overall research process divides into two distinct stages. First, we identified relevant attack vectors and related attacks on blockchain systems by conducting an SLR. Second, we discuss the resulting overview of attack vectors and derive a comprehensive IS research framework and agenda for the cybersecurity of blockchain-based systems under consideration of existing research agendas.

The main objective of the SLR is to produce a comprehensive summary of attacks against blockchain systems and resulting attack vectors. We follow the widely accepted approach by Webster & Watson (2002) to conduct our SLR. Fig. 1 illustrates the SLR process with its individual stages. As an initial step, we extracted search terms from the research question, specifically *attack*, *blockchain*, and *system*. We further refined our list of search terms by including insights from existing attack overviews (Averin & Averina, 2019; Li et al., 2020; Morganti et al., 2018; Shrivas et al., 2020). These overviews frequently use the terms *vulnerabilities, threats*, and *issues* closely related to attacks. We also excluded the terms *smart contract* and *cryptocurrency*, as we found in initial searches that these terms are almost exclusively used in conjunction with the term *blockchain* in articles. Furthermore, we deliberately excluded the terms *distributed ledger technology* or *DLT*, as this study's focus is to provide in-depth insight into blockchain-oriented attacks. This approach allows the study to be more concise. We created a Boolean search string based on these terms, which we applied to search the databases for titles, abstracts, and keywords.

Subsequently, we identified appropriate databases for our search. We selected the ACM Digital Library, IEEE Xplore, and arXiv to cover papers with a technical focus, and AISel and Web of Science (WoS) to cover relevant IS journals and conferences specifically. WoS is a meta-database and, thus, covers multiple databases indexing IS literature, such as Elsevier. This approach lead to the inclusion of five databases, returning 5332 results using the identified search string. We deliberately considered both journal publications as well as conference proceedings for our SLR, as research on blockchain is still in its infancy and evolving quickly (Rossi et al., 2019). Thus, much work is published at conferences. Furthermore, conferences are common outlets for publication in the computer science discipline. The search process was conducted between July and August 2020. We did not limit the database queries in terms of publication date.

We performed several steps to filter the relevant data from the identified literature. During the title and abstract screening, we excluded all non-English articles and literature dealing with non-blockchain DLT. This pre-screening resulted in a total number of $n = 291$ articles, on which we performed in-depth text screening. For the final analysis ($n = 161$), we only included articles that specifically deal with attacks on existing blockchains and did not consider attacks on merely conceptional systems.

Subsequently, we constructed a systemization of the identified attacks by systematically ordering the identified attacks along attack vectors of a generic blockchain technology stack. The development of this systemization was conducted highly iteratively. Following Nickerson, Varshney, & Muntermann (2013), a systemization has to be concise, robust, comprehensive, and explanatory. Therefore, the research team continuously discussed and revised the preliminary systemization until the given requirements were satisfactorily met.

By analyzing commonalities, characteristics and specificities across the identified attacks and attack vectors, we derive a comprehensive research framework for IS research on the cybersecurity of blockchain

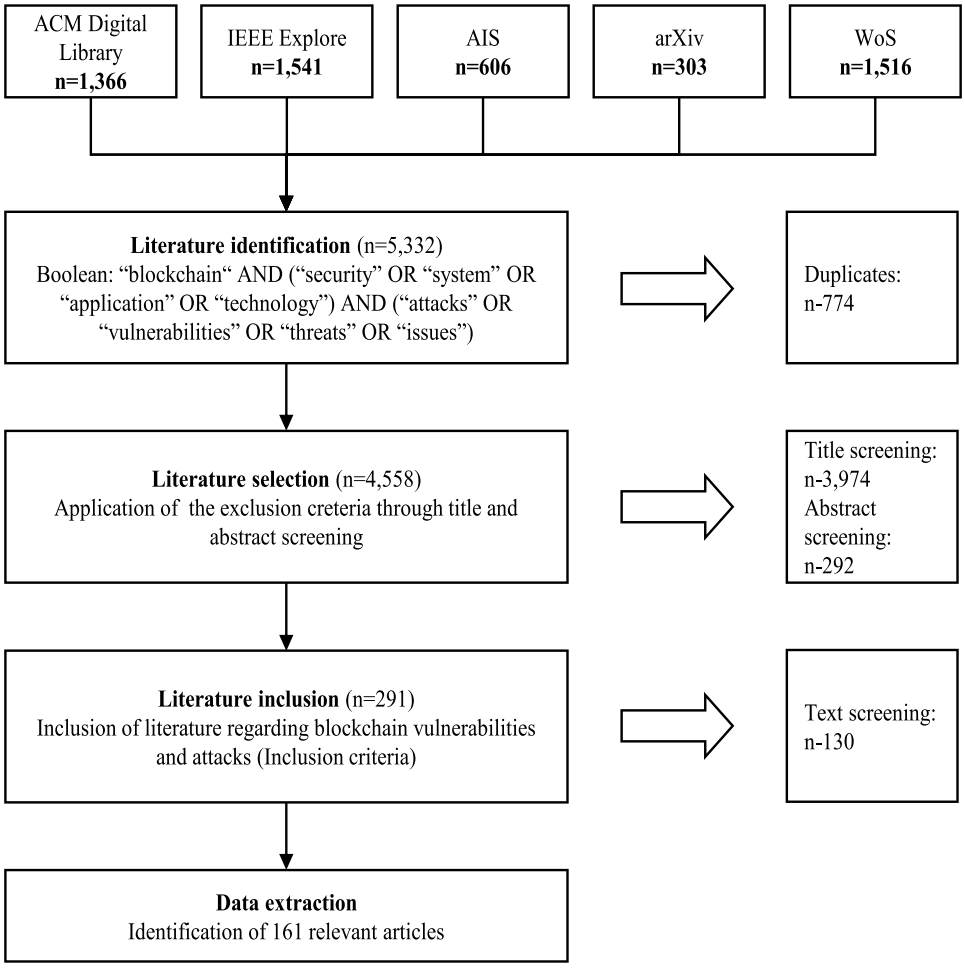


Fig. 1. SLR approach.

systems. In doing so, we take insights from existing research frameworks into account.

Along this conceptual research framework, we propose a research agenda offering fruitful avenues for IS researchers aiming to shed light on perspectives on the cybersecurity of blockchain-based systems.

4. Results

4.1. Consolidation of attacks and identified attack vectors

This study analyzes 161 articles published between 2013 and August 2020. The full results can be found under Schlatt, V., Guggenberger, T., Schmid, J. & Urbach, N. (2021). A more descriptive and attack-centred analysis of the identified attacks is available under (Guggenberger, Schlatt, Schmid, & Urbach, 2021). Even though Bitcoin went live in 2009 already, it took four more years for the first articles analyzing the security of blockchain-based systems to emerge. After the first significant attacks on blockchain-based systems, e.g., Mt. Gox (Feder et al., 2017), caused a stir, publications of scientific papers on blockchain security increased rapidly until 2020. The peak is currently in 2019, with 70 publications. Considering the distribution of articles, we identify that the number of conference proceedings doubled from 2018 to 2019. The total number of journal articles even tripled in that timeframe. This observation demonstrates the increasing research in the field of blockchain cybersecurity. Furthermore, the rising number of journal articles indicates that the research converges toward a higher maturity level. We extracted a total of 87 attacks out of the literature.

We derive a comprehensive systemization of these attacks along generic attack vectors in blockchain-based systems in a next step (see Fig. 2). We explicitly include all types of blockchain technology in our scope. In an iterative process, we subsequently analyzed and sorted the 87 attacks derived from literature along different criteria. These initially included the attacker's goal, the resulting implications of attacks, commonalities in the attacks' conduct, and others. We applied several categorizations and followed the guidelines by Nickerson et al., (2013) to define ending conditions for our categorization process. Thus, the research team continuously discussed and added attacks to different categories, until a concise, robust, comprehensive, and explanatory, systematization was identified (Nickerson et al., 2013). After several sorting rounds, we found that assigning attacks along the generic technology stack of blockchain-based systems produces a selective and exclusive systematization wherein each attack is uniquely assigned to a specific attack vector. We build upon existing representations (Ismail & Materwala, 2019; Pay, 2017; Saad et al., 2020) to derive a generic blockchain technology stack consisting of five layers. In Fig. 2, we denote the number of unique attacks identified per attack vector below the respective attack vector.

The *P2P network* represents the basic layer for data storage and exchange between nodes of any blockchain system. The second layer contains the *consensus mechanism* of a blockchain system, a protocol for achieving consensus on the system's current state between the network nodes. The *virtual machine (VM)* and the respective *programming language* of a blockchain system constitute the third layer and attack vector in our systemization. It contains the components responsible for writing, translating, and executing application logic. Building upon these layers, the application logic represents the fourth attack vector and subsumes

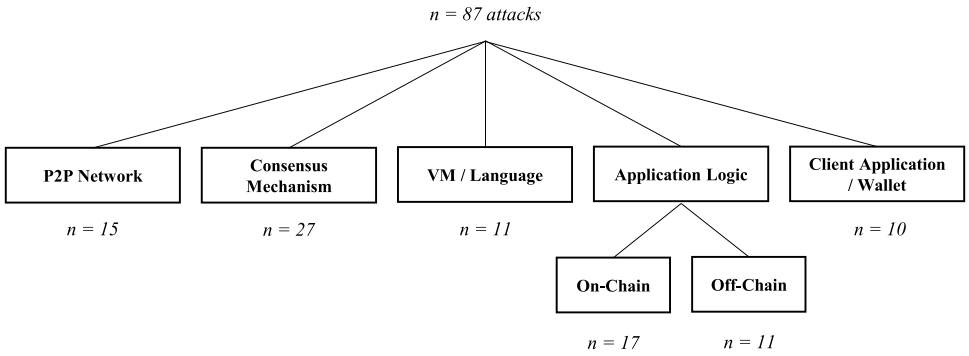


Fig. 2. Attack vectors and identified attacks.

smart contracts and off-chain programs responsible for implementing application logic. We divided this vector into two different sub-vectors. Attackers can either attack the *on-chain application logic* by exploiting vulnerabilities in smart contracts deployed on the blockchain or attack the *off-chain application logic* on connected applications. In general, users employ *client applications/wallets* to interact with blockchain systems, which constitute a further attack vector in the blockchain technology stack. From a superordinate perspective, the attack vectors can be broadly classified into *blockchain infrastructure*, subsuming the P2P network, consensus mechanism, VM, and *blockchain applications*, including the application logic and wallets.

4.2. Overview of the identified attack vectors

The first attack vector subsumes attacks on the *P2P network*. This attack vector relates to the communication between nodes within the network. Attacks in this category are often not specific to blockchain systems but rather relate to generic communication network attacks. Examples of such attacks are distributed *denial of service (DDoS) attacks* or *domain name system (DNS) attacks*. During a *DDoS attack* on blockchain systems, a distributed network of attackers floods the blockchain system with transactions of small amounts in a short period, which occupy the storage of the following blocks (Saad et al., 2020). As a result, the attacker can launch other attacks, like double spending. The *routing attack* poses another risk explicitly aimed at blockchains' *P2P networks*. Thereby, the attacker initially parts the network's users into separate groups and afterward tampers the messages between them, thereby withholding information from each group (Apostolaki, Zohar, & Vanbever, 2017). As a result, attackers can achieve a fork into two chains, increasing the chance of a successful double spend. In total, we subsume 15 attacks under the attack vector *P2P network*.

The second attack vector constitutes the *consensus mechanism*. Different consensus mechanisms with different vulnerabilities exist. However, the proof-of-work consensus mechanisms of Bitcoin and Ethereum remain the most popular and widely examined instances. Attacks on blockchain systems' consensus mechanism mostly characterize as malicious exploitations of the consensus mechanisms' inherent and deliberate design. The *51% attack* on the proof-of-work consensus mechanism is a prominent example. A (group of) miner(s) possess(es) more than 50% of the system's hash rate, allowing them to mine new blocks and thus decide which transactions are included therein (Sayeed & Marco-Gisbert, 2019). This attack can be achieved through withholding a privately mined chain of valid blocks from the public and releasing it before the public chain gets as long as the private instance (Sayeed & Marco-Gisbert, 2019). Paying other miners for writing empty blocks, known as *Goldfinger attack* (Kroll, Davey, & Felten, 2013), is another malicious attack regarding the consensus mechanism, especially applicable to the proof-of-stake consensus mechanism (Wang, Wang, Cao, Li, & Xiong, 2019a) and focused on the human factor of cybersecurity. Another exemplary elaboration of this attack vector is the *race attack*, whereby a merchant does not wait for confirmation before accepting an attacker's transaction of funds. Meanwhile, the attacker (potentially a malicious miner) creates a second block containing a transaction with the same transaction data but is directed to another address controlled by himself. The attacker then hopes that the merchant accepts the first transaction while the second block is validated first, entailing the invalidity of the first transaction to the merchant (Saad et al., 2020). Most attacks on the consensus mechanism of blockchain systems target the canonical-chain rule (i.e., longest chain in Bitcoin and Greedy Heaviest Observed Subtree (GHOST) in Ethereum) and build upon the stochastic nature of consensus mechanisms in common public blockchain systems. In the final systemization, we assigned 27 attacks to the *consensus mechanism*, stressing the relevance of this attack vector.

The layer of the *VM* and inherent *programming language* is responsible for the change of state in blockchain systems. The *VM* is responsible for translating the business logic, written with a particular *programming language*, to computer instructions so that regardless of the environment, the results are deterministic (Hirai, 2017). In this layer, we mainly identified attacks resulting from bugs in implementing a blockchain system's VM and programming language. Therefore, attacks on program functions only belong in this group if the functions' implementation differs from the official documentation. In case the function is implemented correctly but used in an insecure way, we considered this attack to be part of the on-chain application logic group. An appropriate example is the *short address attack*, which exploits an Ethereum VM vulnerability regarding wallets ending to "0" digits. If the attacker executes a purchase through a smart contract with a precise balance and removes the last 0 of the address, the virtual machine adds the missing 0 without having the *buy function* checking the sender's (= attacker's) address (Saad et al., 2020). Subsequently, the attacker's address' balance multiples by 256 each time they execute the purchase. We identified 11 attacks on this attack vector.

The fourth attack vector covers attacks on the *application logic* built upon blockchain system infrastructures, usually deployed by third parties. We distinguish between *on-chain application logic* and *off-chain logic*. Smart contracts, which are directly deployed and executed on a blockchain system, are examples of *on-chain application logic*. The *off-chain application logic*, in contrast, connects users with applications running directly on the blockchain system. Smart contracts are typically written by users and not an inherent part of the blockchain protocol or client and, thus, differ from the *VM/ language*. Once enshrined in a validated block, the smart contract code cannot be modified subsequently (Moubarak, Filiol, & Chamoun, 2016). For example, the *reentrancy attack* exploits a vulnerable smart contract and, hence, the *on-chain application logic*. In this attack, an incautious user can lose all their Ether temporarily saved in a smart contract to an attacker if they do not update the contract's balance before sending Ether (Chen et al., 2020). The off-chain attack vector contains attacks exploiting weaknesses introduced on a layer on top of a blockchain system. For example,

during a *refund attack*, the attacker evades the P2P communication network by feigning cancellation of an order as man-in-the-middle and exploiting the vulnerability that users accept refunds over off-chain communication channels (e.g., e-mails). Consequently, the merchant sends the refunds to the man-in-the-middle-attacker instead of the customer (McCorry, Shahandashti, & Hao, 2016). In summary, we assigned 16 attacks to *on-chain application logic* and 11 attacks to *off-chain application logic*.

The last attack vector concerns the *client application/wallet*. Please note that distinct blockchain systems make different use of the word client and wallet. This article regards the wallet as the cryptographic vault containing cryptographic keys while the client makes use of the wallet and manages connections to the blockchain system. The users of blockchain applications and their wallets pose a considerable security risk. *Phishing* is a generic attack on information systems but also of particular relevance to blockchain-based systems (Hasanova, Baek, Shin, Cho, & Kim, 2019). Another attack is particularly relevant for the Ethereum ecosystem, which often makes use of the Remote Procedure Call (RPC) API to implement DApps. In the case of an unprotected RPC connection, any user could directly connect to the client to perform arbitrary functions. This situation is especially critical when the client has unlocked the wallet, exposing access to the user's private keys (Bui, Rao, Antikainen, & Aura, 2019). We added 8 attacks to this attack vector. Again, in this category, generic attacks on IT systems are prevailing, such as *social engineering attacks*, exploiting vulnerable implementations of cryptography, and others.

5. Research agenda

5.1. Research framework for blockchain cybersecurity

The literature review demonstrates the rising number of articles examining blockchain vulnerabilities and attacks. We assume that this increase in interest is related to the increasing penetration of blockchain systems within diverse application areas. The higher the entrusted value within a blockchain system, the higher the risk of loss, and, therefore, the higher the need for a better understanding of vulnerabilities and the resulting cybersecurity risk. To account for this need, we derive a comprehensive research framework for the cybersecurity of blockchain-based systems from the analysis of attacks on such. Based on this framework, we infer a comprehensive research agenda for IS.

The derived research framework (Fig. 3) entails the main entities and relationships involved in cybersecurity incidents in blockchain-based systems. We developed the respective framework in an incremental manner by conceptualizing existing blockchain research frameworks based on insights gained from analysing the attacks identified in our literature review (Chapter 4). In line with generic research frameworks for blockchain, we therefore divide the entities relevant for research on the cybersecurity of blockchain-based systems into a *human* and an *IT* fraction (Rossi et al., 2019). Thus, we take a socio-technical perspective on failures of IS (Bostrom & Heinen, 1977) to derive our framework, because blockchain-based systems must be understood as socio-technical systems (Ehrenberg & King, 2020). We identify three entities on the human side: users of blockchain applications (which often serve as an entry point and victim for cybersecurity incidents), developers of blockchain-based systems (responsible for creating many attack opportunities and safeguarding blockchain-based systems), and attackers (a dimension added particularly in the context of research on the cybersecurity of blockchain-based systems). The IT side is divided into the underlying blockchain infrastructure, such as the Ethereum platform, and blockchain applications running on top of the protocol (Rossi et al., 2019). The former can often show inherent weaknesses relevant for cybersecurity on a protocol-level, which can only be countered by interdisciplinary approaches (as discussed below). The latter show more "traditional" weaknesses and can benefit from existing approaches to cybersecurity. As evident from the analysed attacks, reciprocal effects characterize the relationships between the entities in the cybersecurity research framework.

On the one hand, *users* use and thereby impact the security of blockchain-based applications and perceive their level of security. On the other hand, *blockchain applications* constrain and influence the actual and perceived security of their users. Likewise, *developers* design, implement, and change blockchain-based systems, entailing both *blockchain applications* and the *blockchain infrastructure* they are built upon, and thereby influence their security properties. In contrast, the IT of blockchain-based systems enables and constrains developers in their options for implementing security features. *Attackers* play a central part in the cybersecurity research framework for blockchain, as they are involved in all cybersecurity incidents. The attackers are characterized by a reciprocal relationship with both users and developers, as well as blockchain applications and blockchain infrastructure: On the one hand, attackers exploit both users and developers as important attack vectors. On the other hand, they often introduce and exploit direct vulnerabilities on a technological level. Both the IT as well as the human entities constrain and influence the behavior of attackers. The impact of bilateral relationships between two entities on other entities and their relationship to each other introduces additional complexity. Each of the entities in the framework and their complex relationships offer fruitful avenues

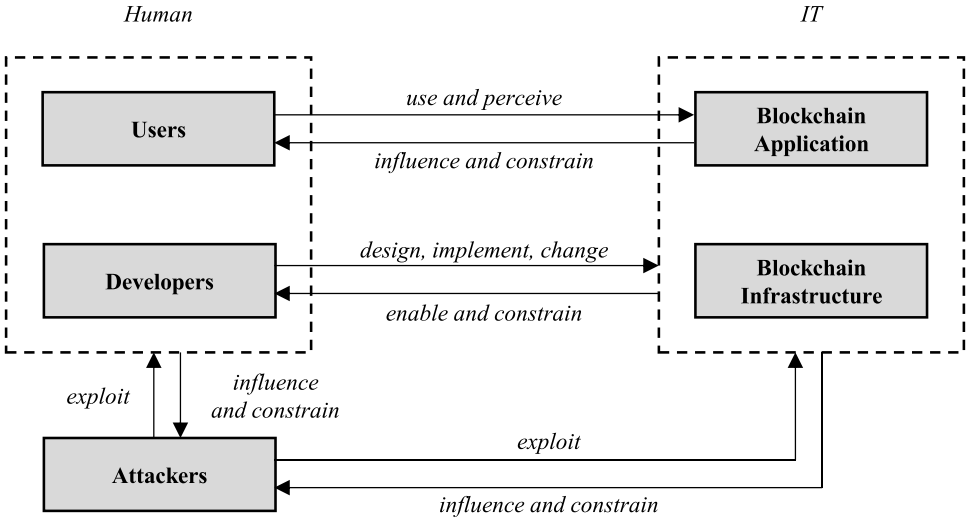


Fig. 3. Blockchain cybersecurity research framework.

for future research. Thus, we develop relevant research propositions (*Pn)*, each aligning with one or more elements in the framework (Hughes et al., 2019).

P1: *The more users are aware and educated about the security of blockchain-based systems, the less cybersecurity incidents induced by users will occur.*

The skills and values of users have an impact on the success or failure of IS (Bostrom & Heinen, 1977). In the realm of cybersecurity, this can reflect in the awareness and education about cybersecurity of specific systems. Research indicates that improvement of these factors will lead to improved security behaviour of IS' users (Li et al., 2019), which may not serve as an entry point as often as a result. We propose that this relationship is present in blockchain-based systems, too, and urge research to evaluate the relevant circumstances. This research proposition focuses on the *users* and *blockchain applications* entities in the research framework.

P2: *Goal-oriented design of blockchain-based systems will positively influence the security-relevant behaviour of their users.*

The behaviour of users can not only be influenced by education and raising awareness, but also through the design of systems. Best practices from the realm of cybersecurity show that mechanisms such as a requiring Two-Factor-Authentication can increase the cybersecurity of systems' users (Ciolino, Parkin, & Dunphy, 2019). We posit, that this aspect is relevant for the design and development of blockchain-based systems, too. More knowledge about users and their perceptions of security-relevant design choices, as well as a detailed analysis of attacks on blockchain-based systems involving users, will lead to design of more secure systems. This research proposition focuses on the *users* and *blockchain applications* entities.

P3: *Incentives to design secure blockchain-based systems will lead to a higher focus on security by their developers.*

As socio-technical systems, the attitudes and reward systems of humans involved in the development and use of blockchain-based systems need to be aligned with the purposes of the IS (Bostrom & Heinen, 1977). We propose that the adequate design of such reward systems and incentives may serve as a motivator for the secure design of blockchain-based systems. For example, financial rewards for finding security issues in the codebase of blockchain-based systems, may incentivize developers to focus on cybersecurity, as do financial losses in the case of incidents (for example, if tokens in a blockchain system belong to their developers). This research proposition focuses on the *developers* and *IT* entities.

P4: *Increased availability of open source software components for blockchain-based applications will lead to more secure software development.*

Although disputed, open source software is regularly considered as an approach for improving the security of software (Hoepman & Jacobs, 2007). Especially in the realm of blockchain technology, where software is regularly developed by different individuals or scattered across organizations, it is important to be able to audit code independently. Standardized and tested open-source components, such as the ERC-721 token interface, may serve as way for more individuals and organizations to develop secure blockchain-based applications, that have been transparently audited by experts. This research proposition focuses on the *developers* and *IT* entities.

P5: *The correlative interaction between humans and blockchain-based systems will lead to new attack vectors to be exploited.*

IS' success as well as failure is characterized by a reciprocal relationship between the socio and the technical parts (Bostrom & Heinen, 1977). Several attacks identified offer illustrative examples for this relationship: phishing attacks involve users as attack vectors in (technologically) secure systems (Hasanova et al., 2019). Goldfinger attacks, on the other hand, involve the developers or maintainers of blockchain-based systems (Kroll et al., 2013). We suppose that more human-centred attacks will occur, while technological security advances. This research proposition focuses on the *human* element.

P6: *A rising number of small-scale blockchain-based systems will lead to more attacks focused on entire networks.*

Important parts of any blockchain-based system build upon scale for improved security. For instance, 51%-attacks become more feasible, as the computing power of the network decreases. Successful attacks from the recent past indicate the importance of this aspect. Concurrently, the number of blockchain networks and applications keep rising. We, therefore, suppose that the number of attacks affecting entire networks increases with this development. This research proposition focuses on the *IT* element.

5.2. Research agenda for blockchain cybersecurity

An interdisciplinary perspective on cybersecurity of blockchain-based systems is central to the proposed research framework. While blockchains are highly automated systems, they must still be understood as socio-technical systems (Ehrenberg & King, 2020). Especially in the realm of cybersecurity, humans play a vital role. From our literature review, we conclude that particularly a socio-technical perspective is lacking in current studies. A majority of the identified papers focus solely on the technical aspects of blockchain security and only few researchers extend this purely technical perspective. For example, the major studies identified in our literature review, which provide an overview of multiple attacks, all cluster these attacks by means of technical categories (Averin & Averina, 2019; Homoliak et al., 2019; Li et al., 2020; Morganti et al., 2018; Saad et al., 2020; Shrivas et al., 2020). We identified no study taking a perspective focusing exclusively on human aspects of cybersecurity. Against this background, building upon the previously developed research framework and propositions, we propose future research avenues along the derived research framework. Table 1 summarizes the proposed research agenda.

The relationship between users and blockchain applications offers various opportunities for research. Users are a vulnerable gateway for attacks on blockchain-based systems. In contrast to exclusively technological agents, humans seldom act deterministically, making it difficult to identify effective countermeasures. General IT/IS security research has long since identified humans as an essential topic of interest (Ghafir

Table 1
IS research agenda for blockchain cybersecurity.

Entity	*Proposed Blockchain Cybersecurity Research Avenues for IS*
User	• *Which attacks on blockchain-based systems are induced by users and what are effective countermeasures?* • *How do users perceive the security of blockchain applications?* • *How to educate and train users to use blockchain applications securely?*
Developer	• *How to design secure software development processes for blockchain technology?* • *What are the socio-technical implications of developers becoming attackers, such as in the Goldfinger attack?* • *What is the impact of the open-source software culture in the realm of blockchain technology on cybersecurity?*
Attacker	• *What motivates attackers of blockchain-based systems?* • *Which goals do attackers of blockchain-based systems pursue?* • *How can data science help in identifying and preventing attacks on blockchain-based systems?*
Blockchain Application	• *How does the design of blockchain applications influence the security-related behaviour of their users?* • *How to design blockchain applications perceived as secure?*
Blockchain Infrastructure	• *Which differences in cybersecurity risk arise from different instantiations of blockchain technology?* • *Which actual risks are associated with attacks on blockchain infrastructure?* • *How to design and evaluate secure consensus mechanisms?*

et al., 2018). In the realm of blockchain, a corresponding research question might be *which attacks on blockchain-based systems are induced by users and what are effective countermeasures?* As our literature review reveals, phishing attacks are present in blockchain systems, too (Hasanova et al., 2019). In this regard, *how to educate and train users to use blockchain applications securely* could be a corresponding research avenue worthwhile pursuing. Offering opportunities for experimental research, the question of *how users of blockchain applications perceive their level of security* might be of interest. Similar endeavors were already conducted regarding the notion of trust in blockchain by users (Marella, Upreti, Merikivi, & Tuunainen, 2020; Ostern, 2018), but are lacking regarding the security aspects.

The opposite relationship between blockchain applications and users offers corresponding avenues for IS research. *How to design blockchain applications perceived as secure* and *how does the design of blockchain applications influence the security-relevant behavior of their users* may be interesting research questions for design science research (Gregor & Hevner, 2013). Answering the first question is essential for the widespread dissemination of blockchain technology in society, as a positive perception of security is a fundamental requirement for the acceptance of the technology (Saad et al., 2020). The answer to the second question can help reducing the cybersecurity risk originating from users, which we identify as under-researched in currently available studies.

Developers design, implement, and change blockchain IT (encompassing both infrastructure and applications). In this light, we again emphasize the socio-technical aspect of cybersecurity attacks on blockchain systems and their respective countermeasures. Erroneous smart contract implementations described in the papers identified in our literature review, e.g., The DAO smart contracts (Mehar et al., 2019) or those exploited through Multiple Withdrawal Attacks (Rahimian, Eskandari, & Clark, 2019), can lead to significant cybersecurity threats, which are exacerbated through the tamper-resistant nature of blockchain technology. Thus, the question of *how to design secure software development processes for blockchain* arises. Initial research in this field has already been conducted (Destefanis et al., 2018). Furthermore, developers can also act voluntarily as cybersecurity threats, e.g., in Goldfinger attacks (Kroll et al., 2013). The *socio-technical implications of attacks such as the Goldfinger attack* might serve as a future field of research, as the motivation of maintainers to attack their own system remains blurry. Furthermore, open-source software development is an integral element of most major blockchain projects. It is also regularly considered as a way to improve software security (Hoepman & Jacobs, 2007). Nevertheless, the impact of open-source software development on cybersecurity is a controversial topic in the academic discourse (Lawton, 2002; Payne, 2002; Schryen, 2011). The *impact of the open-source software culture in the realm of blockchain technology on cybersecurity* might therefore be an interesting research area for the interdisciplinary IS research community.

A central but so far underrepresented element in research on the cybersecurity of blockchain-based systems are attackers. Each attack on an IT system is associated with a motivating goal of the attacker (Howard & Longstaff, 1998). To ensure comprehensiveness, we cover an extensive range of attacks on different types of blockchain-based systems but acknowledge that attackers' factual goals may vary. Therefore, if an attacker aims to compromise a Bitcoin wallet to steal funds, only a subset of the identified attacks may be relevant. *Identifying and interpreting attackers' motivation and goals* may, thus, serve as a fruitful opportunity for future research and aid in a better understanding of cybersecurity of blockchain-based systems. The study by Morganti et al. (2018) already characterizes attacks by the types of attackers likely to perform them, while initial research on the reward expectations of attackers performing double spend attacks has pointed another way in this direction (Ramezan & Cyril, 2020). From an interdisciplinary perspective, *applying and evaluating methods from fields such as data science to identify and prevent attacks on blockchain-based systems* seems like a sensible option to extend the current research landscape. Several papers in the realm of cryptocurrencies show the potential of applying data science methods in blockchain ecosystems (Sun Yin et al., 2019; Yin and Vatrapu, 2017).

The IT components of blockchain systems, namely the blockchain infrastructure and blockchain applications, incorporate technical security features and thereby enable and constrain developers in designing and implementing secure solutions. Due to the technology's inherent properties, blockchain-based systems materialize differently from regular IT systems. We note that certain attacks, such as the 51%-attack, are only relevant in systems employing specific consensus mechanisms or wallets. As a result, researchers could *compare different instantiations of blockchain technology regarding their cybersecurity risk*. Furthermore, it is essential to note that exploits of blockchain-based systems are often less severe on an application-level compared to exploits in the blockchain infrastructure. The P2P network, the consensus mechanism, as well as the VM are globally distributed and, thus, accessible to all legitimate network participants, resulting in a different risk level. Providing more context regarding the risk associated with attack vectors and attacks could offer more guidance on the secure design of blockchain-based systems, an aspect which currently only few studies cover (Li et al., 2020; Morganti et al., 2018). We provide a first systemization of attacks in this paper, but future research could *measure the risk associated with certain attack vectors and attacks on blockchain-based systems* to offer more context, for example, using proven modelling techniques such as attack trees (Mauw & Oostdijk, 2006). Consensus mechanisms are at the heart of blockchain technology and provide opportunities for several attacks illustrated in the results of our literature review (Saad et al., 2020; Sayeed & Marco-Gisbert, 2019; Wang et al., 2019a). As our SLR shows, most attacks on blockchain-based applications target the consensus mechanism. *How to design and evaluate secure consensus mechanisms* might offer a promising research field for the interdisciplinary IS community, as consensus mechanisms often rely on economic and social theory rather than purely technical knowledge.

This study offers future research directions, too. The comprehensive body of literature on attacking blockchain-based systems compiled through our literature review provides opportunities for various meta-analyses. For instance, empirical research could connect the attacks with their factual occurrences, thus helping to improve risk assessment and studying actual impact beyond theory. By applying, evaluating, and improving the proposed research framework, future research may also help in better understanding the socio-technical nature of cybersecurity in blockchain-based systems and beyond. Furthermore, the systematization regarding criticality of attacks on specific parts in the blockchain technology stack, which have already been touched upon and are discussed in detail below, could be empirically evaluated and further refined.

6. Discussion

In the following section, we provide a synthesis and discussion of our research considering the originally proposed research question. Subsequently, we discuss the resulting theoretical and practical implications as well as limitations and future research directions.

Our research question centred around the identification of attacks on blockchain-based systems and the resulting implications for research on the cybersecurity of such. Considering the initial motivation for our research, stating that IS research majorly describes blockchain-technology as being particularly secure, our results show that a multitude of attacks on blockchain-based systems exists. Thus, we contradict this common conception in IS literature. We observe in our SLR that research describing attacks mainly originates from the computer science and software engineering domains, while IS research seems to have a less critical view of the topic. This aspect might result from the positive public reception of blockchain technology, which led IS researchers to focus on the opportunities by the technology rather than the threats.

Likely due to originating from a technology-oriented research

community, most existing research on the cybersecurity of blockchain-based systems revolves around technical aspects. Thus, the socio-technical perspective proposed in our research framework for IS extends the problem space by putting human actors stronger into presence. Applying the proposed framework might therefore require shifting the focus of research and practice on blockchain from technical aspects of attacks to human aspects of cybersecurity, thus representing the "socio" facet. Considering this notion in hindsight, alternative approaches to structuring the attacks identified in the SLR arise. Instead of focusing on the attacks' targeted technology layer of a blockchain-based application, it might be fruitful to structure attacks along socio-technical criteria. For instance, each attack is launched with a motivating goal (Howard & Longstaff, 1998). Structuring attacks along the attacker's motivation can aid in researching and defining mitigation strategies more comprehensively. Depending on the type of blockchain-based application offered, a respective structure allows to identify relevant privacy-related attacks, financially motivated attacks and so on. Combining these insights with knowledge on the operating domain of the respective application and its technical set-up, employing a socio-technical structure can aid in identifying relevant attacks and mitigation strategies more precisely.

Taking a socio-technical perspective on research on cybersecurity of blockchain-based systems also paves the way for applying multi-disciplinary research methods and knowledge from non-technical research domains. Generic IS research focused on blockchain-technology largely involves exploratory and case-based research methods (Hughes et al., 2019). By proposing a socio-technical IS research framework for blockchain-cybersecurity, we suggest applying research methods from domains beyond traditional IS research, such as experiments, which can aid in understanding human aspects.

6.1. Theoretical contributions and implications

To interpret the results of our SLR and infer a comprehensive research agenda, we take a socio-technical perspective as proposed in the seminal work by Bostrom & Heinen (1977). Scholars recently urged IS researchers to put more emphasis on this theoretical stance (Suprateek, Chatterjee, Xiao, & Elbanna, 2019). Bostrom & Heinen (1977) offer a theoretical lens on IS failure, which understands IS as consisting of "two jointly independent, but correlative interacting systems – the socio and the technical" (Bostrom & Heinen, 1977, p. 17). As a result, the design of any well-functioning system must reflect this bond. Through our analysis of existing attacks on blockchain-based systems, we contribute an agenda for IS research on the cybersecurity of such. We posit that related research must respect both socio and technical aspects in understanding attacks and their results. Yet, the current state of literature often solely focuses on technical aspects. For example, users' skills (Bostrom & Heinen, 1977) do have an impact on their security-relevant use of blockchain-based systems, which is evident in the success of phishing attacks and similar attacks. Furthermore, adequately designed reward systems (Bostrom & Heinen, 1977) may aid in incentivizing developers to focus on security-related aspects. In blockchain-based systems, this idea is reflected in several consensus mechanisms or events such as pre-market coin offerings for developers already. Furthermore, the authority structures of an information system (Bostrom & Heinen, 1977), which are often non-hierarchical in blockchain systems (Beck et al., 2018), can have an impact on security as well. So far, the respective structures appear to have been mainly discussed in the context of governance considerations.

6.2. Implications for practice

The derived research framework and its theoretical grounding have a practical impact, too. We propose that the interplay of the individual components in the blockchain technology stack and the relevant attacks for each resulting layer lead to different impacts on and involvement of the human and IT actors within the research framework. Fig. 4 illustrates these interrelations and their implications. We divide the technology stack derived in Fig. 2 into three layers, for each of which specific attack types prevail. The affected as well as the primarily involved entities in the attacks, which we describe in our research framework, differ for each layer.

Functionally, *client applications and wallets* provide interfaces for users to interact with blockchain-based applications. Thus, attacks on this layer have a direct impact on users (sometimes individual, as in phishing attacks, and sometimes on all users of a specific technical artifact, such as a wallet). As our analysis shows, users also serve as an entry point for attackers, and thereby become actively involved in attacks. The *on-chain logic* translates user inputs into transactions on the blockchain network. Thus, the elements represent the logic of entire applications, or even classes of applications. Therefore, attacks on this layer can affect entire applications, such as the attack on the DAO, and vulnerabilities can affect entire classes of applications, such as integer overflow attacks present in versions of the Ethereum VM. Given this context, attacks on blockchain *networks* can affect the security of all users and applications. For instance, a successful 51%-attack, which lately occurred in smaller networks, offers the attacker the possibility to change the content of any transaction in the blockchain.

The affected elements indicate that attacks on different layers have effects of different magnitude. While attacks on the client level mainly impact individuals, attacks on the layers below may have an impact on entire applications or networks. The relevant attack vectors usually differ in this regard. Therefore, we posit that practitioners need to evaluate the security and risks of their blockchain-based applications according to the layers presented. In this context, it is important to consider which layers of the technology stack are within the control of the respective practitioner and choose the technological set-up accordingly. For example, public and permissionless networks may not be under control of individual or entities that can be influenced, which is why the security of their design is dependent on others, as is dealing with attacks. However, the impact of an attack may be large, as 51%-attacks show. On the other hand, specific interfaces as well as applications can be maintained by individual practitioners, allowing for more fine-grained control by individual parties. Understanding which attacks are relevant for each layer, and which measures can be taken to control these, is vital for designing and offering secure blockchain-based applications.

Adhering to the structure proposed, we highlight three specific recommendations for practitioners, which reflect our socio-technical perspective: First, strictly analyze the users of your applications to determine the risk arising from attacks targeting the individual level. The resulting insights may aid in evaluating cybersecurity risks from users as attack vectors, in protecting and educating users, and in determining the business risks from specific blockchain applications regarding legal and other aspects. Second, leverage blockchain-specific software security libraries, such as OpenZeppelin,[1] to support your developers in implementing secure on-chain logic. As research from established cybersecurity domains indicates, securely designed software artifacts aid software developers in building more secure applications (Georgiev et al., 2012). Third, design or choose the underlying blockchain network according to the security needs of the assets involved in your services offered. For instance, this recommendation might result in considering the monetary costs of utilizing public permissionless networks (Lockl et al., 2020) in relation to their potentially higher levels of security, or evaluating the privacy requirements of data contained, which might lead to considering private permissioned networks.

6.3. Limitations and future research

Our research is not without limitations. In the following, we

[1] https://openzeppelin.com/

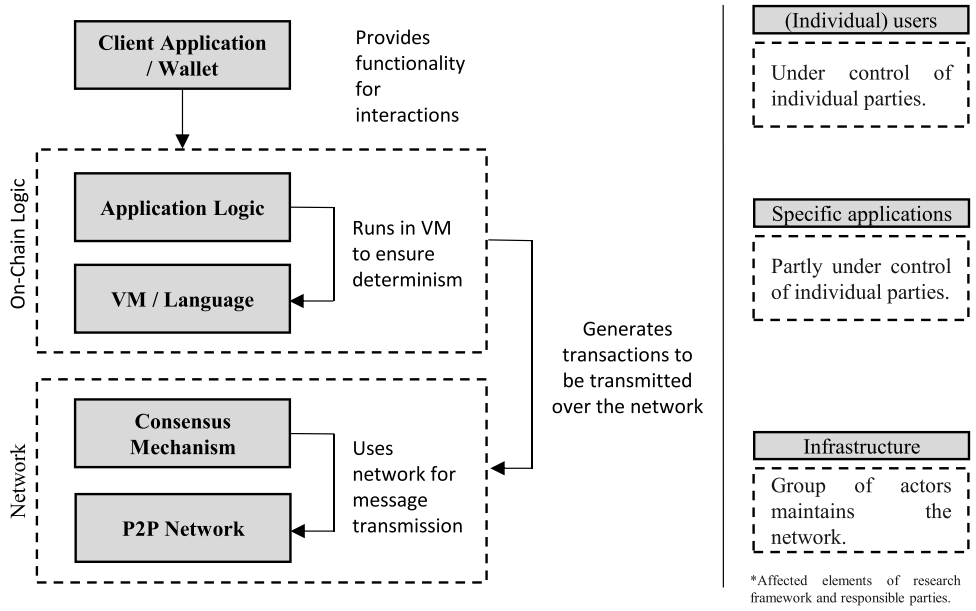


Fig. 4. Affected elements and responsible actors of attacks on technological layers.

highlight three shortcomings and potential resolutions to be addressed by future research. First, we aim to provide a comprehensive IS research agenda for the cybersecurity of blockchain-based systems by analyzing existing attacks. As a result, we cover various blockchain implementations and blockchain types, including public and private blockchains, for our SLR. However, most of the literature mainly focuses on popular public blockchains, e.g., Ethereum or Bitcoin. Adapting the research framework to private blockchain systems might result in some changes, as attack vectors may differ, for example, through the fact that all network nodes are known and trusted. Second, the research on blockchain cybersecurity is quickly evolving. Thus, the proposed research agenda may not be representative in the future. We aim to address this limitation by proposing a generic research framework, along which future research agendas can be developed. Furthermore, we have also included literature published at conference proceedings to account for the quickly evolving and immature research field. However, this implies that some review processes for work taken into account may not have been comprehensive. Third, blockchain research is highly interdisciplinary and the respective technologies must be understood as socio-technical systems. We tried to address this fact in our research framework and agenda. Nevertheless, we only sparsely propose research questions for relevant fields of science outside of the IS realm, such as psychology, sociology, or economics.

It is important to note that this research paper offers a comprehensive overview of attacks and cybersecurity research on blockchain-based systems at a certain point in time. Much of the attention on the topic was originally motivated by cryptocurrencies and the rising amount of value they represented. As a result, research on cybersecurity of blockchain-based systems was also mainly concerned with cryptocurrencies. Yet, more recent trends such as decentralized finance and non-fungible tokens might shift the majority of (financial) value held in blockchain-based systems, thus attracting more attention by attackers. While the respective applications essentially build upon the same technology as cryptocurrencies, the targeted attack vectors might shift towards smart contracts for example, rather than network infrastructure. Thus, this and future research must be viewed in a temporal context.

7. Conclusion

Blockchain-based systems become increasingly valuable targets for cybercrime due to the rising amount of value stored in respective systems. However, researchers and practitioners alike lack a comprehensive and structured overview of existing attacks and a directive discussion of resulting implications. Employing an SLR approach, we analyze literature on cybersecurity aspects of blockchain technology to extract 87 relevant attacks. We structure those attacks and derive a framework for IS research on the cybersecurity of blockchain-based systems. Along this research framework, we infer future research avenues and illustrative research questions.

This article's contribution is threefold: First, we provide a comprehensive and structured overview as well as analysis of attacks on blockchain-based systems derived from literature. Second, we contribute a framework guiding future research in the field of blockchain cybersecurity from an IS perspective. Third, we derive a comprehensive research agenda suggesting corresponding research avenues.

The security of IT systems is under constant change. This observation is especially true for the quickly developing blockchain ecosystem. Short lifecycles and the introduction of new features offer new opportunities for attackers to find exploitable vulnerabilities. Researchers and developers alike put much effort into fixing these exploits. A multidisciplinary approach is vital in developing secure blockchain-based systems for the future and IS research can play an important role in this endeavor. The ever-ongoing race between developers and attackers ensures that research on the security of blockchain-based systems remains an essential topic for the future.

CRediT authorship contribution statement

Vincent Schlatt: Conceptualization; Methodology; Validation; Data curation; Writing – original draft; Writing – review & editing; Visualization; Project administration. **Tobias Guggenberger**: Conceptualization; Methodology; Validation; Data curation; Writing – original draft; Visualization. **Jonathan Schmid**: Investigation; Data curation; Writing – original draft; Visualization. **Nils Urbach**: Writing – review & editing; Supervision.

Declaration of interest

N/A.

References

Ali, O., Ally, M., Dwivedi, Y., & others. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management, 54*, Article 102199.

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing attacks on cryptocurrencies. *IEEE Symposium on Security*, 375–392.

Averin, A., Averina, O., (2019). Review of blockchain technology vulnerabilities and blockchain-system attacks, International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 1–6.

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). *Blockchain technology in business and information systems research*. Springer.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*(10), 1–1034.

Berger, S., Bürger, O., & Röglinger, M. (2020). Attacks on the industrial internet of things – Development of a multi-layer taxonomy. *Computers & Security, 93*, Article 101790.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly, 1*, 17–32.

Bui, T., Rao, S. P., Antikainen, M., & Aura, T. (2019). Pitfalls of open architecture. *EuroSys*, 1–6 (Conference).

Bumblauskas, D., Mann, A., Dugan, B., & Rittmer, J. (2020). A blockchain use case in food distribution: Do you know where your food has been? *International Journal of Information Management, 52*, Article 102008.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Privacy-preserving data certification in the internet of things: Leveraging blockchain technology to protect sensor data. *Journal of the Association for Information Systems, 20*(9).

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys, 53*(3), 1–43.

Ciolino, S., S. Parkin, P. Dunphy (2019). Of two minds about two-factor: Understanding everyday 5FIDO6 U2F usability through device comparison and experience sampling. In: Fifteenth Symposium on Usable Privacy and Security (5SOUPS6 2019).

CoinMarketCap, 2022. Top 100 cryptocurrencies by market capitalization. URL: ⟨https://coinmarketcap.com/⟩ (visited on 01/09/2022).

Conti, M., Sandeep Kumar, E., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452.

Destefanis, G., M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, R. Hierons (2018). Smart contracts vulnerabilities: a call for blockchain software engineering?. In: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 19–25.

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research, 58*(11), 3381–3398.

Ehrenberg, A. J., & King, J. L. (2020). Blockchain in context. *Information Systems Frontiers, 22*(1), 29–35.

Feder, A., Gandal, N., Hamrick, J. T., & Moore, T. (2017). The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. *Journal of Cybersecurity, 3*(2), 137–144.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management, 51*, Article 102029.

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological Forecasting and Social Change, 163*, Article 120407.

Georgiev, M., S. Iyengar, S. Jana, R. Anubhai, D. Boneh, V. Shmatikov (2012). The most dangerous code in the world: validating SSL certificates in non-browser software. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 38–49.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986–5002.

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis, Hawaii International Conference on Systems Science (HICSS 2017).

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337–355.

Guggenberger, T., Schweizer, A., & Urbach, N. (2020). Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology. *IEEE Transactions on Engineering Management, 67*(4), 1074–1085.

Guggenmoos, F., J. Lockl, A. Rieger, A. Wenninger, G. Fridgen (2020). How to develop a GDPR-compliant blockchain solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure, 53th Hawaii International Conference on Systems Science (HICSS 2020).

Guggenberger, Tobias; Schlatt, Vincent; Schmid, Jonathan; and Urbach, Nils, "A Structured Overview of Attacks on Blockchain Systems" (2021).https://aisel.aisnet.org/pacis2021/100/.

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management, 29*(2), Article e2060.

Hirai, Y. (2017). Defining the ethereum virtual machine for interactive theorem provers, International Conference on Financial Cryptography, 520–535.

Hoepman, J.-H., & Jacobs, B. (2007). Increased security through open source. *Communications of the ACM, 50*(1), 79–83.

Homoliak, I., S. Venugopalan, Q. Hum, P. Szalachowski (2019). A security reference architecture for blockchains. URL: ⟨http://arxiv.org/pdf/1904.06898v1⟩.

Howard, J. D., & Longstaff, T. A. (1998). *A common language for computer security incidents*. Albuquerque, NM (US): Sandia National Labs.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management, 49*, 114–129.

Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry, 11*(10), 1198.

Jensen, T., Hedman, J., & Henningsson, S. (2019). How TradeLens delivers business value with blockchain technology. *MIS Quarterly Executive, 18*(4), 221–243.

Kroll, J.A., I. C. Davey, E.W. Felten (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. Proceedings of WEIS, 11.

Lawton, G. (2002). Open source security: opportunity or oxymoron? *Computer, 35*(3), 18–21.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24.

Li, X., P. Jiang, T. Chen, X. Luo, Q. Wen (2020). A survey on the security of blockchain systems. URL: ⟨http://arxiv.org/pdf/1802.06993v3⟩.

Lindman, J., V. K. Tuunainen, M. Rossi (2017). Opportunities and risks of blockchain technologies-A research agenda. In: Proceedings of the 50th Hawaii International Conference on System Sciences.

Liu, Z., & Li, Z. (2020). A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management, 52*, Article 102059.

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things (IoT) Ecosystems: Design principles for blockchain-based IoT applications. *IEEE Transactions on Engineering Management, 67*(4), 1256–1270.

Magazzeni, D., McBurney, P., & Nash, W. (2017). Validation and verification of smart contracts: A research agenda. *Computer, 50*(9), 50–57.

Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Electronic Markets, 30*, 1–13.

Mauw, S., & Oostdijk, M. (2006). Foundations of Attack Trees. *Information Security and Cryptology*, 186–198.

McCorry, P., Shahandashti, S. F., & Hao, F. (2016). Refund attacks on Bitcoin's payment protocol. *International Conference on Financial Cryptography*, 581–599.

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., … Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology (JCIT), 21*(1), 19–32.

Mendling, J., Weber, I., Aalst, W., vom Brocke, J., Cabanillas, C., Daniel, F., & Zhu, L. (2018). Blockchains for business process management - Challenges and opportunities. *ACM Transactions on Management Information Systems*.

Miede, A., Nedyalkov, N., Gottron, C., König, A., Repp, N., & Steinmetz, R. (2010). A generic metamodel for IT security attack modeling for distributed systems. *International Conference on Availability*, 430–437.

Modgil, S., & Sonwaney, V. (2019). Planning the application of blockchain technology in identification of counterfeit products: sectorial prioritization. *IFAC-PapersOnLine, 52*(13), 1–5.

Morganti, G., E. Schiavone, A. Bondavalli (2018). Risk assessment of blockchain technology, Eighth Latin-American symposium on dependable computing (LADC), 87–96.

Moubarak, J., E. Filiol, M. Chamoun (2016). On blockchain security and relevant attacks, IEEE Middle East and North Africa Communications Conference (MENACOMM), 1–6.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems, 22*(3), 336–359.

Ostern, N. (2018). Do you trust a trust-free transaction? Toward a trust framework model for blockchain technology. *International Conference on Information Systems (ICIS)*.

Pay, S. (2017). Towards common blockchain architecture — an "ISO OSI for blockchain" primer. URL: ⟨https://medium.com/@scanpayasia/towards-common-blockchain-architecture-an-iso-osi-for-blockchain-primer-778db4e5b35c⟩ (visited on 08/26/2020).

Payne, C. (2002). On the security of open source software. *Information Systems Journal, 12*(1), 61–78.

Peters, G. W., E. Panayi (2015). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In: Banking beyond banks and money, pp. 239–278.

Pournader, M., Shi, Y., Seuring, S., & Koh, S. L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research, 58*(7), 2063–2081.

Rahimian, R., Eskandari, S., & Clark, J. (2019). Resolving the multiple withdrawal attack on ERC20 tokens. *IEEE European Symposium*, 320–329.

Rahouti, M., Xiong, K., & Ghani, N. (2018). Bitcoin concepts, threats, and machine-learning security solutions. *IEEE Access, 6*, 67189–67205.

Ramezan, G., & Cyril, L. (2020). Analysis of proof-of-work-based blockchains under an adaptive double-spend attack. *IEEE Transactions on Industrial Informatics, 16*(11), 7035–7045.

Risius, M., & Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering, 59*(6), 385–409.

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems, 20*(9), 14–1403.

Rupasinghe, T., F. Burstein, C. Rudolph (2019). Blockchain based dynamic patient consent: a privacy-preserving data acquisition architecture for clinical data analytics. In: International Conference on Information Systems 2019.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. H., & Mohaisen, D. (2020). Exploring the attack surface of blockchain: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 22*(3), 1977–2008.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9*(9), 1788.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 53–74.

Schryen, G. (2011). Is open source security a myth? *Communications of the ACM, 54*(5), 130–140.

Schuetz, S., & Venkatesh, V. (2020). Blockchain, adoption, and financial inclusion in India: Research opportunities. *International Journal of Information Management, 52*, Article 101936.

Schweizer, A., V. Schlatt, N. Urbach, G. Fridgen (2017). Unchaining social businesses: Blockchain as the basic technology of a crowdlending platform, 38th International Conference on Information Systems (ICIS).

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering, 62*(6), 599–608.

Shrivas, M. K., T. Y. Dean, S. S. Brunda (2020). The disruptive blockchain security threats and threat categorization, First International Conference on Power, Control and Computing Technologies (ICPC2T), 327–338.

Suprateek, S., Chatterjee, S., Xiao, X., & Elbanna, A. R. (2019). The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance. *MIS Quarterly, 43*.

Sun Yin, H. H., K., Langenheldt, M., Harlev, Mukkamala, R. R., & Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. *J. Manag. Inf. Syst, 36*(1), 37–73.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*(2), 147–156.

Schlatt, V., Guggenberger, T., Schmid, J. & Urbach, N. (2021). Appendix: Overview of attacks. URL: ⟨https://doi.org/10.5281/zenodo.4399697⟩ (visited on 12/29/2020).

Wang, H., Wang, Y., Cao, Z., Li, Z., & Xiong, G. (2019a). An overview of blockchain security analysis. *Communications in Computer and Information Science, 970*, 55–72.

Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., & Wang, F.-Y. (2019b). Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems, 6*(5), 870–878.

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52*, Article 102090.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii–xxiii.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Yin, H. S. and R. Vatrapu (2017). "A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning". In: 2017 IEEE International Conference on Big Data (Big Data), pp. 3690–3699.

Zhu, L.-H., Zheng, B.-K., Shen, M., Gao, F., Li, H.-Y., & Shi, K.-X. (2020). Data security and privacy in Bitcoin system: A survey. *Journal of Computer Science and Technology, 35*(4), 843–862.

Ziolkowski, R., G. Miscione, G. Schwabe (2020). Exploring decentralized autonomous organizations: Towards shared interests and 'Code is Constitution', 41st International Conference on Information Systems (ICIS).