A Structured Overview of Attacks on Blockchain Systems

Completed Research Paper

Tobias Guggenberger
FIM Research Center,
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
Wittelsbacherring 10,
95444 Bayreuth, Germany
tobias.guggenberger@fim-rc.de

Vincent Schlatt
FIM Research Center,
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
Wittelsbacherring 10,
95444 Bayreuth, Germany
vincent.schlatt@fim-rc.de

Jonathan Schmid
FIM Research Center,
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
Wittelsbacherring 10,
95444 Bayreuth, Germany
jonathan.schmid@fim-rc.de

Nils Urbach
FIM Research Center,
Project Group Business & Information Systems Engineering of the Fraunhofer FIT,
Frankfurt University of Applied Sciences
Nibelungenplatz 1,
60318 Frankfurt am Main, Germany
nils.urbach@fim-rc.de

Abstract

Blockchain systems become increasingly attractive targets for cybercrime due to the rising amount of value transacted in respective systems. However, researchers and practitioners alike lack a comprehensive overview of existing attacks and a directive discussion of resulting implications. Employing a structured literature review, we analyze academic research concerning malicious attacks on blockchain systems. We extract 87 relevant attacks and structure those using the attack tree notation. Our results show that the academic discourse revolves mainly around the analysis of a few individual attacks, and most publications deal with attacks on either Bitcoin or Ethereum. We further find that most attacks target the on-chain application logic component (smart contracts) of the blockchain technology stack as well as consensus mechanisms. A majority of attacks are mitigable, and socio-technical components play an important role in both attacks and applying effective countermeasures.

Keywords: Blockchain, IT Security, Structured Literature Review, Attack Tree

1 Introduction

Blockchain systems become increasingly relevant in business and society. While the technology originally gained traction as the backbone of the digital currency Bitcoin, a multitude of applications ranging from supply chain management (Guggenberger et al. 2020), energy markets (Mengelkamp et al. 2018) to the Internet of Things (Lockl et al. 2020) and decentralized finance (Chen and Bellavitis 2020) exists today. These applications aim at leveraging the inherent characteristics of the technology, such as decentralization, tamper-resistance, and transparency (Schweizer et al. 2017).

As a result, blockchain 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 330 billion as of November 2020 (CoinMarketCap 2020). Besides, many blockchains facilitate smart contracts, allowing individuals and organizations to implement arbitrary business logic on a decentralized infrastructure. Consequently, such systems can hold crucial information for business processes. For example, the German Federal Office for Migration and Refugees develops a blockchain-based system for managing highly sensitive refugee identities along the asylum process (Guggenmoos et al. 2020).

This ever-rising value stored in blockchain systems creates increasingly attractive targets for attackers. Recent years reported several prominent cybercrimes on respective systems. Furthermore, blockchain-based systems have become increasingly complex. Promising new decentralized finance applications make extensive use of complex smart contract structures. For instance, the MakerDao ecosystem comprises several thousand lines of code, which makes open-source due diligence highly challenging (Maker 2020). 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 et al. 2017).

Despite the relevance of such cybersecurity incidents, there is no comprehensive overview and discussion of existing research concerning the respective attacks. As our literature review indicates, existing research is highly selective regarding the scope of attacks and that they are often not structured adequately. However, researchers and practitioners alike should holistically consider the security threats on blockchain-based systems to design, develop, and evaluate applications based on such systems. To fill this research gap, we aim to answer the following question:

What are known attacks on blockchain systems and how can they be structured?

We answer this question by collecting and analyzing attacks on blockchain 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 using the attack tree (AT) notation (Mauw and Oostdijk 2006). Based on the findings of the literature review and the structuring, we eventually discuss the resulting implications. Thus, we aim to contribute to the discussion on the current state in the literature concerning attacks and security threats on blockchain-based systems to the academic discourse and propose resulting future research opportunities. As a result, this article also aids practitioners in building secure blockchain applications by providing a holistic overview and context of existing attacks.

The remainder of this paper is structured as follows. Section 2 sets the necessary foundations, covering blockchain and related IT security research. Section 3 describes the research method, while Section 4 presents the findings of the literature review and the resulting AT. Section 5 provides a comprehensive discussion of the resulting implications on the design of secure systems based on blockchain. The following Section 6 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 systems, several different concepts of blockchain arose over the past decade. A popular categorization by Peters and Panayi (2015) distinguishes between public blockchains where transactions are publicly visible and private blockchains where transactions are only visible to authorized parties. Furthermore, permissioned blockchains allow anyone to participate in the P2P network and validate transactions, while permissionless systems retain this right to authorized parties exclusively. Along these architectural dimensions, different consensus mechanism alternatives to the computationally intensive and, thus, relatively inefficient proof-of-work in Bitcoin emerged (Sedlmeir et al. 2020). While some of these 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 the 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. Practical applications of smart contracts include global container shipping processes (Jensen et al. 2019), second-hand car sales (Zavolokina et al. 2020), and P2P energy trading (Mengelkamp et al. 2018). Advanced ideas on the use of respective smart contracts involve creating nexuses of smart contracts creating decentral autonomous organizations (Beck et al. 2018). In a famous security incident, the supposedly first instance of such an organization became the victim of an attacker exploiting a code vulnerability in a smart contract, eventually leading to the loss of significant funds and the decline of the organization (Dhillon et al. 2017).

2.2 Security aspects of blockchain technology

Information security generally aligns along the CIA triangle comprising the cybersecurity goals of confidentiality, integrity, and availability (Whitman and Mattord 2011). Research lately extended these foundational goals of information security to include authenticity, accountability, auditability, trustworthiness, non-repudiation, and privacy (Berger et al. 2020).

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 intentionally unauthorized target by carrying out several planned steps to achieve their ultimate goal (Howard and Longstaff 1998). Along the way, attackers execute individual steps and employ various 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 and 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 IT security. 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.

The research took up the lack of coherent overviews of attacks. Saad et al. (2020) provide an overview of attacks on blockchain technology by assigning attacks to three pre-determined attack surfaces related to system components: the P2P communication system, the blockchain data structure, and blockchain applications. The authors identify and describe 17 differing attacks. Similarly, Conti et al. (2018) and Homoliak et al. (2019) survey the security of blockchain-based systems. The former work concentrates mainly on presenting threats regarding Bitcoin's security and privacy and its proof-of-

work consensus mechanism. Thereby, the authors provide a discussion of state-of-the-art countermeasures to these threats but focus solemnly on a specific instantiation of blockchain technology. Homoliak et al. (2019) provide a comparably comprehensive overview of blockchain security and additionally define a reference architecture model, which they analyze in the course of the article, detailing weaknesses and potential points of attack. The authors provide four attack surfaces and model attacks and groups thereof in graphs to identify causal relationships between attacks. In sum, the authors identify 29 attacks. Chen et al. (2020) present an overview of vulnerabilities and attacks on Ethereum smart contracts, again, a specific instantiation of a blockchain system. The results are thus limited to the Ethereum blockchain and lack attacks regarding other consensus mechanisms. A further approach to structuring attacks is given by Zhu et al. (2020). The respective authors systematize attacks on Bitcoin's blockchain, concentrating on the target surface of data by assigning attacks to three clusters: data privacy attacks, data availability attacks, and data consistency attacks. Another related publication by Rahouti et al. (2018) provides a further account of multiple attack vectors on blockchain systems. This work is also limited to attacks related to Bitcoin's proof-of-work consensus mechanism.

Recently, more generic overviews of attacks on blockchain systems emerged sporadically (Averin and Averina 2019; Li et al. 2020; Morganti et al. 2018; Shrivas et al. 2020). While aiming to provide a comprehensive overview, the respective papers are nevertheless limited in their scope. The paper identifying the largest amount of attacks presents 49 attacks (Shrivas et al., 2020). Also, the methodical approach of the respective papers is rather untransparent and, therefore, lacks reproducibility. For example, while Li et al. (2020) offers a systematic review of identified attacks, they do not further describe how they gathered their data (i.e., state the used search strings or databases). As a result, the informational value about the state of the literature shows limitations.

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 developed an AT to structure and present the results of our SLR.

The main objective of the SLR is to produce a comprehensive summary of attacks against blockchain systems. In particular, we follow the widely accepted approach by Webster and Watson (2002) to conduct our SLR. We extracted search terms from the research question in the first step, specifically *attack*, *blockchain*, and *system*. We further refined our list of search terms by including insights from existing attack overviews (Averin and 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 information systems journals and conferences. This approach leads to the inclusion of five databases that returned 5,332 results using the identified search string. 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 conceptional systems. Figure 1 illustrates the SLR process with its individual steps.

Based on the literature review findings, we construct an AT to structure the attacks with regard to our research question. ATs were initially introduced to systematically understand and formalize attacks on

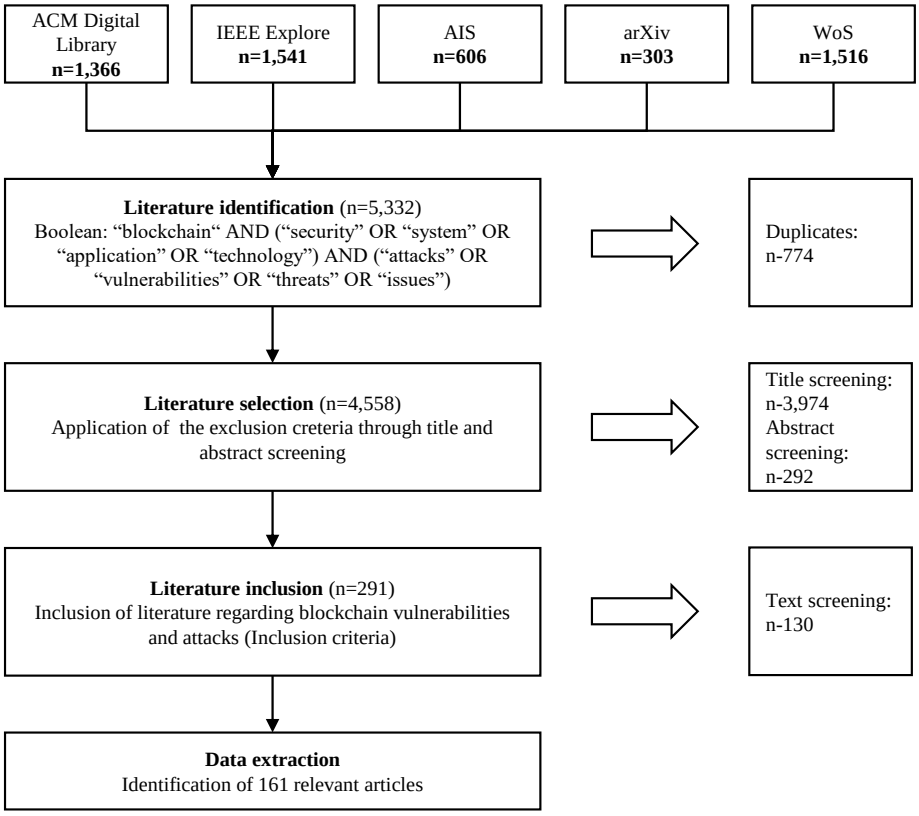

Figure 1. SLR approach.

an IT system (Byres et al. 2004). ATs are widely accepted and have been applied to evaluate the security of online banking systems (Edge et al. 2007), SCADA systems (Byres et al. 2004), and homeland security (Edge et al. 2006). Formally, an AT is a hierarchical graph in which nodes represent attacks on a system. The starting point and root node of an AT is the global goal of an attacker. To achieve the global target, the successful accomplishment of sub-goals is usually necessary. These sub-goals form sub-nodes in the graph. Both AND nodes and OR nodes can be distinguished. For AND nodes, all sub-goals must be achieved to reach a node of the higher level. Such AND nodes are identifiable through conjunctive arcs in the tree. At OR nodes, the attacker must achieve either of the sub-goals to reach the next level (Mauw and Oostdijk 2006; Schneier 2000).

We constructed the individual branches of the AT by systematically adding the identified attack vectors from the literature to the graph. The development of the AT was conducted highly iteratively. Following (Nickerson et al. 2013), a systemization has to be concise, robust, comprehensive, and explanatory. Therefore, the research team continuously discussed and revised the preliminary AT until the given requirements were satisfactorily met.

4 Results

4.1 Descriptive analysis

This study analyzes 161 articles published between 2013 and August 2020 (see Figure 2). The full results can be found under (The Authors 2021). Even though Bitcoin went live already in 2009, it took four more years for the first articles to analyze the security of the blockchain systems to emerge. After the first significant cyber-attacks on blockchain systems, e.g., Mt. Gox, caused a stir (Feder et al. 2017), publications of scientific papers on blockchain security increased rapidly until 2020. The peak is currently in 2019, with 70 publications. We extracted a total of 87 attacks out of the literature.

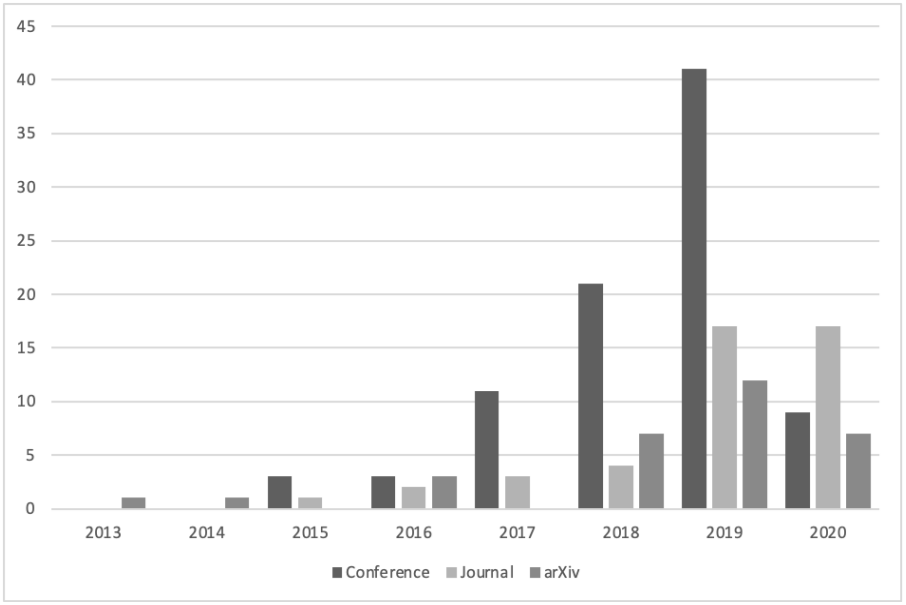

Figure 2. Publications per year in the selected literature.

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 security. Furthermore, the rising number of journal articles indicates that the research converges toward a higher maturity level. At the time of writing this study, there are currently more journal articles published in 2020 than articles from conference proceedings.

Only 7% of all articles provide a comprehensive survey on blockchain security. Most articles (93%) mention 10 attacks and less, focusing on specific instances of blockchain systems or specific attacks in detail. We further found that 62% of all attacks (n=55) are documented less than 5 times. However, literature discusses some attacks particularly frequently, including *double spending* (n=39 papers), *selfish mining* (n=33 papers), or *DDoS attacks* (n=31 papers), which are also often used as an umbrella term for a large number of more specific sub-attacks.

4.2 Consolidation and attack tree development

In the following section, we describe the construction and the resulting structure of our AT. Consolidating the attacks identified through our literature review, we first specified a global attacker goal as the root of our AT. To produce a comprehensive and generic overview of attacks, we defined this goal as *Maliciously attack a blockchain system*. We explicitly include all types of blockchain systems 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. After several sorting rounds, we found that assigning attacks along the generic technology stack of blockchain systems produces a selective and exclusive AT wherein each attack is uniquely assigned to a specific attack vector. We denote the number of unique attacks identified per attack vector under the respective nodes in our AT. The number of occurrences in literature for each attack is denoted in brackets behind the attack name. We define the global goal's direct sub-goals as attacking individual components of a generic blockchain technology stack. We build upon existing representations (Ismail and Materwala 2019; Pay 2017; Saad et al. 2020) to derive a generic blockchain technology stack consisting of five layers (see Figure 3).

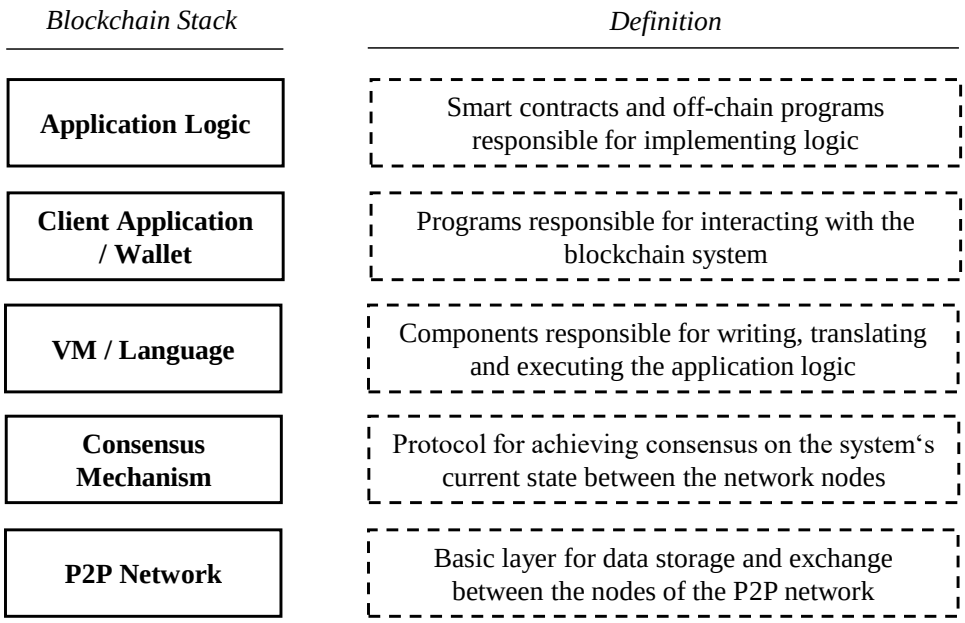

Figure 3. Generic blockchain technology stack.

The *P2P network* represents the basic layer of any blockchain system. The second layer contains the *consensus mechanism* of a blockchain system. The *virtual machine (VM)* and the respective *programming language* of a blockchain system constitute the third layer and attack vector in our AT. Building upon these layers, the logic of blockchain-based applications represents the fourth attack vector. We divided this vector into two different sub-nodes in our AT. Attackers can either attack the *application logic on-chain* 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. We used this classification for the structuring of our AT (see Figure 4).

The first attack node 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, to exploit merchants. The *routing attack* poses another risk explicitly aimed at blockchains' *P2P networks*. Thereby the attacker must accomplish two steps to execute the attack successfully. Initially, the attacker parts the network's users into separate groups and afterward tampers the messages between them, thereby withholding information from each group (Apostolaki et al. 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 sub-goal *Attack the P2P network*.

The second branch constitutes the attack surface of 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. For conciseness, the attack surface could be split into block generation (called mining in Bitcoin) and block validation. The former denotes the process of contributing a new block to the network. The latter comprises the transaction validation by the network by confirming the integrity of the latest block proposed to the system by other peers. However, differentiation between these two mechanisms is often not trivial, and usually, attacks make use of the combination of both. Therefore, we decide not to split the branch up but rather observe attacks on the consensus mechanism holistically. Attacks on blockchain systems' consensus mechanism mostly characterize as malicious exploitations of the consensus mecha-

nisms' inherent and deliberate design. The *51%-majority attack* on the proof-of-work consensus mechanism is a prominent example. A (group of) miner(s) possess(-es) more than 50 percent of the system's hash rate, allowing them to mine new blocks and thus decide which transactions are included therein (Sayeed and 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 and Marco-Gisbert 2019). Paying other miners for writing empty blocks, known as *Goldfinger attack* (Kroll et al. 2013), is another malicious attack regarding the consensus mechanism, especially applicable to the proof-of-stake consensus mechanism (Wang et al. 2019) and focused on the human factor of IT security. 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 AT, 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 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 branch of the AT.

The fourth branch of the attack tree 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* as one sub-branch. 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 et al. 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 sub-goal of the AT contains attacks, which exploit 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 et al. 2016). In summary, we assigned 16 attacks to *on-chain application logic* and 11 attacks to *off-chain application logic*.

The last sub-goal of our AT is called *Attack the client application/wallet*. Please note that distinct blockchains 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 also 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 systems (Hasanova et al. 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 use 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 et al. 2019). We added 8 attacks to this subgoal. Again, in this category, generic attacks on IT systems are prevailing, such as *social engineering attacks*, exploiting vulnerable implementations of cryptography, and others.

5 Discussion

5.1 Findings related to the current state of literature

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 better understanding vulnerabilities.

Through our SLR, we observed that the publication outlets of research on attacks on blockchain systems shifted. While non-peer-reviewed articles published in arXiv initially dominated the total amount of relevant publications, the database only yielded 12 results in 2019, while peer-reviewed journals published 17 articles, and peer-reviewed conferences included 41 articles. This observation indicates a growing maturity of the research field. This aspect becomes even clearer in 2020, when halfway through this year 17 relevant peer-reviewed articles have been published in journals, more than 9 in conference proceedings, and 7 articles on arXiv. Yet, it is worth noting that the drop in conference proceedings in 2020 might be related to the Covid-19 pandemic. Investigating whether a corresponding topical shift exists, for example, whether more attacks on consensus mechanisms alternative to Bitcoin's proof-of-work were discussed in more recent research, would be a fruitful future research endeavor. Particularly the shift in research regarding technical developments in the field of blockchain technology could be of interest in this regard.

Despite the rising number of articles, most papers focus solely on the technical aspects of blockchain security. Only very few researchers deal with attacks on blockchain systems from an interdisciplinary perspective and extend the purely technical IT perspective. While blockchains are highly automated systems, they still must be understood as socio-technical systems (Ehrenberg and King 2020). Humans play a vital role in various ways, either as users overseeing their wallet or as developers creating the fundamental protocols and smart contracts of blockchains. For most of the technical attacks, researchers already propose various countermeasures or simple software fixes. However, the human factor remains a very vulnerable attack surface within many systems. In contrast to exclusively technical problems, humans seldom act deterministically, making it often more difficult to identify effective countermeasures. General IT/IS security research has long since identified humans as an essential topic of interest (Ghafir et al. 2018). Transferring findings from this research field to blockchain security research potentially offers valuable new insights and could help build more secure blockchains and blockchain-based applications.

5.2 Findings regarding the identified attacks

We derive further implications regarding the constructed AT. Each attack on an IT system is associated with a motivating goal of the attacker (Howard and Longstaff 1998). To ensure our results' comprehensiveness, we chose a deliberately broad goal as our AT's root node. Consequently, we cover an extensive range of attacks on different types of blockchain 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 matching attackers' goals on blockchain systems with relevant attacks may, thus, serve as a fruitful opportunity for future research. In this regard, we observe that the financial motivation of attackers on blockchain systems often prevails. Some attacks are specifically focused on obtaining financial values stored in blockchain systems directly, such as the prominent *Double Spend* attacks (39 occurrences) or *Wallet Malware* attacks (5 occurrences), while others indirectly allow obtaining financial values, e.g., through *Selfish Mining* (33

occurrences). Attacks not directly focused on gaining financial values can, nevertheless, have positive financial impacts on the attackers, for example, if they can re-write debt obligations in decentralized finance applications through *Sybil* attacks (34 attacks).

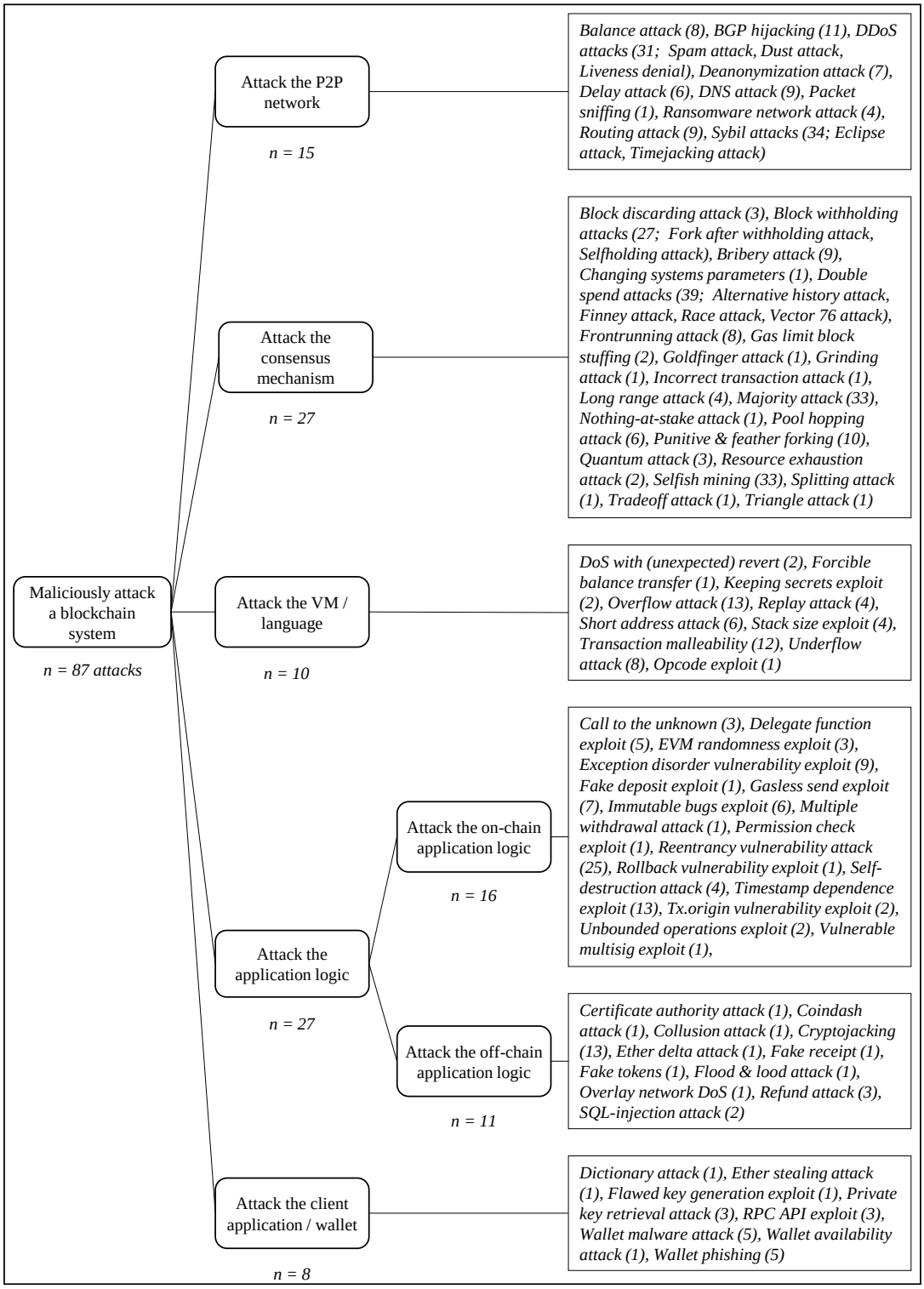

Figure 4. The generic blockchain attack tree.

As some attacks in the AT are only applicable to specific protocols, consensus mechanisms, or even providers of applications, the blockchain system's specific implementation should be considered. On a superordinate level, it is essential to note that vulnerabilities and exploits of client applications and wallets are often less severe on a system-level compared to other components in a blockchain system. The *P2P network*, the *consensus mechanism*, as well as the *VM*, and most of the *application logic* are

globally distributed and, thus, accessible to all legitimate network participants. Such parties could be any user in a permissionless system or at least every node in a permissioned system. Once an attacker finds an exploit in these components, they will be able to attack them directly. In contrast, even though a wallet software might be broken, an attacker still first must gain access to the technical infrastructure of the wallet owner before they can use the exploit. This observation exposes a further possible threat distinction depending on the locality of the attack vector. Furthermore, the susceptibility of specific types of blockchain systems for attacks and the occurrence of attacks on the respective systems may differ.

We further find that some attacks in our AT are inherent to the concept of blockchain, while others are introduced through incorrect implementations. The former includes attacks on certain aspects of consensus mechanisms. Attacks on smart contracts, such as *Multiple withdrawal attacks* (Rahimian et al. 2019), serve as an example of the latter. Therefore, such attacks introduced through incorrect implementations can often be avoided or fixed through mindful software development processes and thorough code reviews. We derive three implications from this observation.

First, we note that some attacks are mitigable, while others are not (at least in specific instances of blockchain systems). Researchers and practitioners should consider this aspect when designing respective systems. As our SLR shows, countermeasures exist for the majority of identified attacks, and many solutions found their way into blockchain implementations. Due to the tamper-resistant nature of blockchain technology, these measures should be incorporated at the design stage. To account for non-mitigable attacks, researchers and practitioners should carefully consider their blockchain system's chosen instantiation according to their goals. For example, some non-mitigable attacks, such as the 51%-majority attack, are only relevant in systems employing specific consensus mechanisms or wallets.

Second, we again emphasize the socio-technical aspect of cybersecurity attacks on blockchain systems and their respective countermeasures. Erroneous smart contract implementations, e.g., that of The DAO smart contracts, can lead to significant security threats. Programmers should be aware of and adequately trained to avoid the respective errors. However, humans can not only serve to mitigate attacks but also as the gateway for attackers. As outlined above, cybersecurity attacks such as *phishing* (Hasanova et al. 2019), resulting in the theft of private keys, are problematic in blockchain environments as well. Strategies to mitigate these should be considered with regard to the training and awareness of users. In summary, the human influence on the security of blockchain systems is relevant both before the deployment of a solution during the development process, and after deployment, on the side of users.

Third, attacks can occur at different levels of the blockchain stack and thus have different effects. For example, a DDOS attack can impact the entire network and disrupt the operations of all participants. Therefore, the impact of such an attack is much more problematic from a network perspective than the theft of a single private key. Accordingly, researchers should focus their efforts on detecting and mitigating attacks that can cause global damage. Attacks on wallets, for example, are considered harmful to the entire network only if they are based on systematic vulnerabilities, e.g., if all wallets in a network are compromised by a code flaw.

6 Conclusion

Blockchain 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 using the AT notation and lead a discussion of the resulting implications.

This article's contribution is threefold: First, we provide a comprehensive and structured overview of attacks on blockchain systems derived from literature. Second, we discuss the resulting implications with regard to the state of research and the socio-technical and technical context of attacks on blockchain systems. Third, we guide practitioners on implementing secure blockchain-based applications by discussing attack vectors concerning mitigability, impact, and attacker motivation. Future research

can now build upon the initial overview set by this publication and extend our discussion with a potential focus on the design of secure blockchain software development and usage, or the interrelations between different attacks and their concrete security impact.

Our research is not without limitations. The AT notation typically envisages a decoration of the graph with attribute values representing the cost or impact of attacks (Mauw and Oostdijk 2006). Furthermore, ATs are extensible to include countermeasures against individual attacks as well (Kordy et al. 2010). More detailed ATs can also contain AND nodes, which might be applicable for individual attacks on blockchain systems (such as routing attacks), implying that one attack serves as a prerequisite for another attack on either the same or a different layer of the blockchain technology stack. Therefore, future research could extend the AT with attribute values for individual attacks and their potential countermeasures to allow for a more fine-grained overview of attacks, their risk potential, and possible countermeasures. As we consulted exclusively academic literature on cybersecurity attacks on blockchain systems, our results might be biased. Hence, future research could include practitioners' perspectives on the construction of a corresponding AT through the involvement of grey literature or expert interviews. Additionally, we chose a generic and rather global attacker goal to construct a maximally comprehensive AT. However, the actual goal of an attacker might be more detailed. As a result, only a sub-set of our identified attacks might be relevant for their particular goal. Thus, we encourage future research to identify common attacker goals and then construct more fine-grained and narrow ATs with respect to these goals.

Our goal was to provide a comprehensive overview of the current state of the literature on the security threats of blockchain systems. Therefore, we did try to cover various blockchain implementations and blockchain types, including public or private blockchains, for our SLR. We identified that most of the literature mainly focuses on popular public blockchains, e.g., Ethereum or Bitcoin, resulting in an overrepresentation of threats on the related systems. Further analyzing the security of private blockchains, therefore, offers an opportunity for future research.

The security of IT systems is under constant development. This observation holds especially true for the very fast 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 solving these exploits. As a result, some attacks of the AT are not present in newer releases of respective blockchain implementations, yet new exploits are likely to appear. 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.

7 References

Apostolaki M, Zohar A, Vanbever L (2017) Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. IEEE Symposium on Security:375–392. https://doi.org/10.1109/SP.2017.29

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, Müller-Bloch C, King JL (2018) Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems 19:1

Berger S, Bürger O, Röglinger M (2020) Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. Computers & Security 93:101790. https://doi.org/10.1016/j.cose.2020.101790

Bui T, Rao SP, Antikainen M, Aura T (2019) Pitfalls of open architecture. EuroSys (Conference):1–6. https://doi.org/10.1145/3301417.3312495

Byres EJ, Franz M, Miller D (2004) The use of attack trees in assessing vulnerabilities in scada systems. Proceedings of the international infrastructure survivability workshop:3–10

Chanson M, Bogner A, Bilgeri D, E. Fleisch, Felix Wortmann (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

Chen H, Pendleton M, Njilla L, Xu S (2020) A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput. Surv. 53:1–43. https://doi.org/10.1145/3391195

Chen Y, Bellavitis C (2020) Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights 13. https://doi.org/10.1016/j.jbvi.2019.e00151

CoinMarketCap (2020) Top 100 Cryptocurrencies by Market Capitalization. https://coinmarketcap.com/. Accessed 17 November 2020

Conti M, Sandeep Kumar E, Lal C, Ruj S (2018) A Survey on Security and Privacy Issues of Bitcoin. IEEE Commun. Surv. Tutorials 20:3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Dhillon V, Metcalf D, Hooper M (2017) The DAO hacked. In: Blockchain Enabled Applications. Springer, pp 67–78

Edge K, Dalton G, Raines R, Mills R (2006) Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security. IEEE Military Communications conference:1–7. https://doi.org/10.1109/MILCOM.2006.302512

Edge K, Raines R, Grimaila M, Baldwin R, Bennington R, Reuter C (2007) The Use of Attack and Protection Trees to Analyze Security for an Online Banking System. 40th Annual Hawaii International Conference on Systems Science (HICSS 2007). https://doi.org/10.1109/HICSS.2007.558

Ehrenberg AJ, King JL (2020) Blockchain in Context. Inf Syst Front 22:29–35. https://doi.org/10.1007/s10796-019-09946-6

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

Ghafir I, Saleem J, Hammoudeh M, Faour H, Prenosil V, Jaf S, Jabbar S, Baker T (2018) Security threats to critical infrastructure: the human factor. J Supercomput 74:4986–5002. https://doi.org/10.1007/s11227-018-2337-2

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)

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 67:1074–1085

Guggenmoos F, Lockl J, Rieger A, Wenninger A, Fridgen G (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)

Hasanova H, Baek U, Shin M, Cho K, Kim M-S (2019) A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Int J Network Mgmt 29. https://doi.org/10.1002/nem.2060

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

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

Jensen T, Hedman J, Henningsson S (2019) How TradeLens Delivers Business Value With Blockchain Technology. MISQE 18:221–243. https://doi.org/10.17705/2msqe.00018

Kordy B, Mauw S, Radomirović S, Schweitzer P (2010) Foundations of attack-defense trees. International Workshop on Formal Aspects:80–95

Kroll JA, Davey IC, Felten EW (2013) The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. Proceedings of WEIS:11

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 67:1256–1270

Maker (2020) MakerDAO. https://github.com/makerdao. Accessed 15 November 2020

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

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

Mehar MI, Shier CL, Giambattista A, Gong E, Fletcher G, Sanayhie R, Kim HM, Laskowski M (2019) Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. Journal of Cases on Information Technology (JCIT) 21:19–32

Mengelkamp E, Gärttner J, Rock K, Kessler S, Orsini L, Weinhardt C (2018) Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied Energy 210:870–880. https://doi.org/10.1016/j.apenergy.2017.06.054

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. https://doi.org/10.1109/ARES.2010.17

Morganti G, Schiavone E, Bondavalli A (2018) Risk Assessment of Blockchain Technology. Eighth Latin-American Symposium on Dependable Computing (LADC):87–96

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

Nickerson RC, Varshney U, Muntermann J (2013) A method for taxonomy development and its application in information systems. European Journal of Information Systems 22:336–359. https://doi.org/10.1057/ejis.2012.26

Pay S (2017) Towards common blockchain architecture — an "ISO OSI for blockchain" primer. https://medium.com/@scanpayasia/towards-common-blockchain-architecture-an-iso-osi-for-blockchain-primer-778db4e5b35c. Accessed 26 August 2020

Peters GW, Panayi E (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

Rahimian R, Eskandari S, Clark J (2019) Resolving the Multiple Withdrawal Attack on ERC20 Tokens. IEEE European Symposium:320–329. https://doi.org/10.1109/EuroSPW.2019.00042

Rahouti M, Xiong K, Ghani N (2018) Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. IEEE Access 6:67189–67205. https://doi.org/10.1109/ACCESS.2018.2874539

Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang DH, Mohaisen D (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey. IEEE Commun. Surv. Tutorials 22:1977–2008. https://doi.org/10.1109/COMST.2020.2975999

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

Schneier B (ed) (2000) Secrets and lies: Digital security in a networked world. John Wiley, New York

Schweizer A, Schlatt V, Urbach N, Fridgen G (2017) Unchaining Social Businesses : Blockchain as the Basic Technology of a Crowdlending Platform. 38th International Conference on Information Systems (ICIS)

Sedlmeir J, Buhl HU, Fridgen G, Keller R (2020) The Energy Consumption of Blockchain Technology: Beyond Myth. Bus Inf Syst Eng 62:599–608. https://doi.org/10.1007/s12599-020-00656-x

Shrivas MK, Dean TY, Brunda SS (2020) The Disruptive Blockchain Security Threats and Threat Categorization. First International Conference on Power, Control and Computing Technologies (ICPC2T):327–338

The Authors (2021) Appendix: Overview of Attacks. https://zenodo.org/record/4613398. Accessed 17 March 2021

Wang H, Wang Y, Cao Z, Li Z, Xiong G (2019) An Overview of Blockchain Security Analysis. Communications in Computer and Information Science 970:55–72. https://doi.org/10.1007/978-981-13-6621-5_5

Webster J, Watson RT (2002) Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26:xiii–xxiii

Whitman ME, Mattord HJ (2011) Principles of information security. Cengage Learning

Zavolokina L, Ziolkowski R, Bauer I, Schwabe G (2020) Management, Governance and Value Creation in a Blockchain Consortium. MIS Quarterly Executive 19:1–17. https://doi.org/10.5167/uzh-178630

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. J. Comput. Sci. Technol. 35:843–862. https://doi.org/10.1007/s11390-020-9638-7