A Survey of Organizational Threats of Blockchain

Tommy Koens

ING
tommy.koens@ing.com

Abstract. Surveying blockchain threats is important as it allows for identification of risks related to blockchain. Existing work provides good systematic surveys of blockchain threats; however, these are incomplete as their focus is on security and privacy threats only. In this research we extend the existing literature by systematically surveying and classifying threats of blockchain. We focus on the threats of blockchain that are not related to security and privacy, and call these organisational threats.

1 Introduction

Blockchain, the technology underpinning cryptocurrencies such as Bitcoin and Ethereum, has been acclaimed to be able to disrupt most industries [7]. This disruption is based on the promise that blockchain eliminates central party risk. For example, the decentralized nature of blockchain may eliminate counter-party risk from transactions [29]. Using blockchain, however, is not without risk. Many threats that could lead to a risk are present in this technology. Identifying these threats is useful because these threats allow for identifying and assessing of the risks of using blockchain. However, such threats have only partially been surveyed. The focus of existing surveys, for example [12] and [22], is on security and privacy threats of blockchains. There clearly is a knowledge gap on surveyed blockchain threats.

In this research we start by introducing some background on public and private blockchains in Section 2. We address the knowledge gap contributing a systematic survey and classification of organisational blockchain in Section 3. We discuss our work in Section 4 and discuss related work in Section 5. Finally, we provide our conclusions in Section 7.

2 Background

In this section we introduce some background on public and private blockchains and their primary properties.

A blockchain is a database which holds some state that is linked to a particular previous state. In general there are two types of blockchains, public blockchains such as Bitcoin and Ethereum and private blockchains such as Corda and Hyperledger Fabric. Primary properties of a public blockchain are that they are:

- **Public**. Anyone can read from the ledger.
- **Permissionless**. Anyone can become a participant and anyone can propose new state changes.

Primary properties of private blockchains are that they are:

- **Private**. Only a limited group of participants is able to read from the ledger.
- **Permissioned**. Only a limited group of participants is able to propose state changes. State changes are proposed by means of voting, as the identity of participants is known in private blockchains.

In both blockchain types participants form a network and reach consensus on the next state of the ledger. State changes can be proposed by sending a transaction, for example, with the intention to issue an change of ownership of tokens. A private cryptographic key allows for proving current ownership of tokens, whereas a public cryptographic key is used as an address to bind the tokens to. Some ledgers support smart contracts (such as Ethereum) whereas other ledgers do not (such as Bitcoin). A smart contract is a piece of software that allows for digital verification or enforcement of an agreement between two or more parties.

3 Classifying and surveying blockchain threats

We surveyed the literature on blockchain threats and classified these threats in two categories. The first category contains the threats that are caused by human behaviour when using blockchain. The second category contains the threats that are caused by blockchain. As stated in Section 1 we exclude security and privacy threats as these already have been surveyed. We summarize our findings in Table 1.

3.1 Threats caused by human behaviour

In this section we address the threats that are caused by human behaviour.

Smart contract as law. Applying smart contracts as law can be considered to be a threat [34]. Smart contracts are agreements written in software code which is executed at a given time or when a trigger appears. On one hand this immutable and irreversible execution of code is a strength of blockchain. However, smart coding errors may lead to unwanted or unexpected behaviour of the smart contract. For example, the DAO hack could be performed due to the smart contract code.

Hard forks The DAO hack ultimately led to a hard fork of Ethereum, namely Ethereum and Ethereum classic. In the former blockchain the chain was reversed to a point before where the DAO hack appeared. In the latter blockchain the hack was accepted, as 'code is law' [17]. Hard forks as such allow the history of the ledger to be altered. This goes against the general idea of a blockchain being immutable. Also, hard forks may create multiple versions of authoritative

Table 1. Survey of blockchain organisational threats

No.	Threat	Sources	Cause
1	Smart contract as law	[34]	Human behaviour
2	Hard forks	[32]	
3	Law and smart contracts	[17]	
4	Different and lack of blockchain regulation	[17] [26]	
5	Insider trading and market abuse	[34]	
6	Design decisions	[24] [13]	
7	Blockchain scalability	[6]	
8	Misapplication of blockchain	[**?**]	
9	Lack of blockchain adoption	[13]	
10	Competitive advantage	[8]	
11	Key person threat	[24] [1]	
12	Increased responsibility on the end user	[17]	
13	Abandoning the blockchain	[6]	
14	Irrevocably storing objectionable content	[24]	
15	Vendor threat	[10]	
16	Customer lock-in	[17]	
17	Energy consumption	[30] [31] [14]	Blockchain
18	No paper based backup	[25]	
19	Illusion of free will	[33]	
20	Lack of interoperability	[10]	
21	Non-compliance to regulation	[10] [8]	
22	Technological evolution	[13], [10], [6]	

data structures. This goes against the idea of a blockchain being a single reliable source of truth [32].

Law and smart contracts. Another threat is the judicial decision to reverse a smart contract for legal noncompliance [17]. The irreversible nature of a public blockchain makes it hard to reverse the execution of a smart contract.

Different and lack of blockchain regulation. To initiate a transaction on a public blockchain a participant must posses some tokens of value (e.g. a cryptocurrency). Even if a participant were only to invoke a smart contract, such a token would be needed as a fee must be paid to include the transaction into the ledger. Transacting with a cryptocurrency may go against a countries legislation as, for example, cryptocurrencies are banned in Bangladesh [17].

Additionally, there exists the threat of an increased responsibility towards the end user. To manage this threat, end users outsource blockchain activities such as key management and wallet management. However, outsourcing such activities introduces new threats. For example, an exchange can simply steal the tokens [26] and it is then hard to revert the tokens to their rightful owner.

Insider trading and market abuse. Zetsche et al. [34] argue that, as all information stored on a public blockchain can be viewed by anyone, it could lead to 'market manipulation or other unfair practices'. As an example, storing re-

cent trades on a public blockchain may lead to front-running competitors or manipulate stock prices.

Design decisions. Design decisions must be made before choosing a blockchain solution. Here, the threat is that the technological solution does not match the use case requirements [24]. A typical example is that of transaction throughput [13]. Current blockchain solutions have limited transaction throughput. Ethereum, for example, can process 15 transactions per second. If, for example, the use case requires more than 15 transactions per second, blockchain is not the best technological choice.

Blockchain scalability Furthermore, Atzori [6] argues that scalability is a threat. Atzori refers to scalability as the feature that anyone that is a miner can join a mining pool. Typically, mining pools offer smaller but frequent rewards towards miners in contrast to a single miner that aims for high rewards. Given the current hashing power in public blockchains, rewarding a single miner will happen approximately every 2 million years (depending on the single miner's hashing power) due to the probabilistic nature of the consensus algorithm [28]. This would lead to centralization due to the decrease of single miners being able to perform the mathematical verification required by the protocol [6].

Misapplication of blockchain. Several papers, for example [13] [21], argue that blockchain can be used to solve particular problems, in particular removing intermediaries. However, it is not clear what the effects are of removing intermediaries. If we assume that there exists a centralisation problem in an industry (e.g. central institutes) current research shows that blockchain may not be the best choice as it solves a particular problem but may render the use case inviable [**?**].

Lack of blockchain adoption. If blockchain were to be used, behaviour change is expected from its participants. Resistant to change may lead to not adopting blockchain [13]. Additionally, moving existing contracts or business documents to a blockchain may hinder the adoption of blockchain, as this migration may take significant time [13].

Competitive advantage. According to Borenstein [8] there exists a threat that industry peers gain a competitive advantage when blockchain is not applied by other peers as blockchain may provide several advantages such as improve operational efficiency, improved transparency, and improve services (e.g. transactions may require a lower fee in banking payment systems). Note that this threat could also be considered an opportunity from the perspective of the industry peer.

Key person threat. Matzutt et al. argue [24] that write access to the code of public blockchains is limited to only a few developers which makes these developers key persons. These developers approve small changes by fiat, and for larger changes community feedback is requested [11]. However, developers may become ill, fail to convince the majority of the community, or may otherwise abandon their activities. This would lead to the loss of a key person capacity and an uncertain future for the blockchain [1].

Increased responsibility on the end user. The lack of a central authority in public blockchains makes that there is an increased responsibility for the end

user, i.e. a participant initiating transactions [17]. Namely, events such as the loss of a private key, the compromise of an account, or user errors could occur. When such an event occurs and no mitigating measures are taken the tokens that are bound to the pubic key are lost.

Abandoning the blockchain. Atzori [6] argues that there exist a risk of the blockchain forking. Here, forking refers to deliberately branching from the main chain, effectively creating a new blockchain. There could be, for example, an unresolved dispute which could lead to such a fork. Even so, such a dispute may lead to the community dismissing the blockchain altogether at any time [6].

Risk of irrevocably storing objectionable content on the blockchain. The blockchain transaction history is hard to re-write which makes that data stored on the blockchain stays on the blockchain, in principle, indefinitely. However, next to transactions it is also possible to write additional content to a blockchain. Matzutt et al. [24] mention content such as copyright violations, malware, politically sensitive content, illegal and condemned content. Storing a blockchain on a device such as a laptop or server would thus also imply storing objectionable content.

Vendor threat. Blockchain initiatives consist of a partnership between multiple organisations and a software vendor that delivers a blockchain solution. There exists the threat of the vendor not being able to deliver results or gain enough financial support [10].

Customer lock-in. The lack of international standards on blockchain could lead to customer lock-in [17]. Here, a customer would become dependent on a vendor for its technology as there are no viable alternative solutions, or it becomes to expensive to migrate to another solution. Note that from the perspective of a vendor this threat could be considered an opportunity.

3.2 Threats caused by blockchain

In this section we address the threats that are caused by blockchain.

Energy consumption. A major current drawback of public blockchains is their energy usage [17], as some corporate institutions aim to comply to an environmental policy. Several studies [30] [31] [14] show that the energy consumption of the Bitcoin network takes on large proportions because of its proof-of-work (PoW) consensus algorithm. A website [2] is dedicated on tracking Bitcoin's energy consumption which in July 2019 equals that of Austria's annual energy consumption. This website also shows that the Bitcoin network is responsible for 0.25% of the global energy consumption. Such energy requirements may be, or may become, too high for a company to participate in a public blockchain as it does not comply with its environmental policy.

No paper based backup. Maurer and DuPont [25] also argues that there is the threat of no paper-based backup archiving the existence or execution of the contracts stored on the blockchain. In case of the blockchain no longer being used, there would be no assurance of contracts stored on the abandoned blockchain being valid.

Illusion of free will. Wright and De Primavera [33] argue that there is a threat in smart contracts (where 'code is law') that may lead to an increase of algorithmic governance. The idea is that smart contracts could suggest a range of partners one should marry, or optimal places where to live. This creates the illusion of free will, as ultimately choices are determined by a network of algorithms [33].

Lack of interoperability. There exists the threat that a blockchains can not interoperate with other technologies. This can be either other blockchain technologies or legacy systems. Although there exist solutions for intra-blockchain interoperability [19], interoperability between blockchain and legacy systems are considered an inhibitor of technological innovation [10].

Non-compliance to regulation. A key property of blockchain is that it represents a ledger of which a copy is stored at multiple nodes. In particular public blockchains, where anyone can join the network and download a copy of the ledger, the ledger is stored globally at multiple nodes. For example, Ethereum nodes are dispersed over at least five continents [5]. This may be a threat as a company may not be compliant to regulations when using blockchain [10] [8]. It would be extremely hard, if not impossible, to manage this data distribution. Additionally, a transaction fee has to be paid each time a smart contract is invoked. This fee is sent to the miner who includes the transaction in a valid block. Before sending the transaction to the network, one does to know which miner will mine the next block. As an example, a block could be mined by a miner in a black-listed country with which no trade is allowed. The effect would be that a company does trade, as the transaction fee from the company is send to the miner in the black-listed country.

Technological evolution. A potential threat lies in the technological evolution. For example, quantum computing may be a threat once it further evolves [13], [10], [6], as digital signatures in current public blockchains will be broken and solving the consensus puzzle can be done twice as fast, giving the attacker a significant advantage over the rest of the miners.

4 Discussion

Current surveys on blockchain threats focus [12] [22] on security and privacy threats, as discussed in Section 2. Our survey shows that there are additional inherent threats when blockchain is applied. None of the research surveyed propose concrete mitigating measures for these threats which can be explained by that for each threat a different type of mitigating measured can be applied. For example, lack of compliance to particular legislation can be avoided by simply deploying the blockchain in a country where the legislation does not apply. There likely will be an overlap in threats for different blockchain initiatives. Here, these initiatives could re-use the mitigating measures related to specific blockchain threats. For example, a company using a blockchain in Europe may have to deal with the GDPR. Other industries can learn from the measures taken to deal with the Compliance threat.

5 Related work

In this section we discuss related work on threats and blockchain.

Crosby et al. [13] argue that blockchain is adopted slowly because of the risk associated with this technology. Charting blockchain threats allows for a systematized approach on mitigating those threats. Our work contributes in a further charting blockchain threats.

Borenstein [8] discusses why banks are experimenting with blockchain from a (bank) risk perspective. This suggest that blockchain can be used to address those risks. Borenstein argues that banks are experimenting with blockchain to address regulatory risks. However, in our work we argue that the public nature of (public) blockchains result in (regulatory) threats. The risks stemming from these threats are hard to mitigate through public blockchains.

KPMG propose a blockchain assessment solution to determine blockchain risks. Their model consist of 10 blockchain risk areas [20]. The model is very high level and no further information is publicly available. Their model contains organisational (e.g. use case relevance), technical (e.g. scalability), and procedural (e.g. permissions management) risk areas. Our survey on organisational threats extend their work as it is more detailed. The only exception is that we did not find any threats related to governance in the blockchain literature. This clearly is an open field for future research.

Deloitte [3] proposes a blockchain risk management framework which includes several risk ares. These ares, however, are a mix of specific and generic risks that apply to blockchain such as regulatory risks and information security risk. Additionally, some risks in their model only apply to specific use cases, such as liquidity risks. In our work we focus on generic threats, leaving out threats of use cases, and we propose a classification of threats (that could lead to a risk) which clearly makes a distinction between specific threats and generic threats.

Homoliak et al. [18] propose a threat-risk model following the ISO/IEC 15408 (Evaluation criteria for IT security [4]) standard. Their model, however, only includes some security and privacy as surveyed by Conti et al. [12] and Li et al. [22] and does not include organisational threats. Their model can be extended with the organisational threats surveyed in our work.

Lindmann et al. [23] propose a research agenda on blockchain. One of the questions they propose is "how to identity and mitigate blockchain threats?". Furthermore, they highlight the need to address blockchain threats. Our work surveys, classifies and analysis organisational threats of blockchain, which allows for addressing the risks stemming from these threats in a structured manner. Furthermore, to understand the risks of blockchain technology, Lindmann et al. [23] propose a distinction between organisational, (business) environmental and technological risks of blockchain for specific use cases. For example, Lindmann et al. include the the cost structure and profit potential of the service that runs on top of the blockchain. Another example is that of market environment by user demand, where competitors offer similar or substitute services [23]. Dilley et al. [16], Brezo and Bringas [9], Moore and Christin [27] discuss several risks from the perspective of Bitcoin, which is use case specific. Dierksmeyer and

Seele [15] survey legal, regulatory and governance threats for cryptocurrencies. Cryptocurrencies are a specific use case where blockchain is used. In our work we focus on the threats of blockchain technology without zooming in on a specific use case. In our work we propose a new classification for general organisational threats, and survey and analyse these organisational threats as we do not focus on use case specific threats of blockchain.

Conti et al. [12] analyse security and privacy threats of Bitcoin specifically. Li et al. [22] assess the security of public blockchains, in particular Ethereum and Bitcoin. In our work we look beyond these security and privacy threats and complement their work with our own survey of organisational threats of blockchain.

6 Future work

The existing literature o blockchain and risk focuses on technology threats of public blockchains. An open path for future research is the identification and classification of technological threats of private blockchains.

As discussed in Section 5 we did not find any blockchain threats related to governance in the literature. Current work on blockchain governance focuses on *how* to achieve decentralized governance. Identifying governance threats for blockchain clearly is an open research question.

As indicated in Section 3 some threats can also be considered an opportunity for using blockchain. Identifying these opportunities as well as determining how they relate to blockchain threats is an interesting path for future research.

In our work we also surveyed organisational threats based on existing literature. Another approach would be the identification of organisational threats by means of analysing blockchain use cases. This could lead to the identification of new threats, as well as the verification on whether or not our survey on organisational threats is complete.

7 Conclusion

In this research we surveyed the organisational threats of blockchain. Our work complements existing work on blockchain threats and can also be used for identifying organisational blockchain risks. Out of scope of our work are security and privacy threats as these already have extensively been surveyed in [12] [22]. Blockchain threat surveys are important as they are a foundation for the identification of blockchain risks.

Furthermore, although there is a strong focus on security and privacy threats by researchers, organisational blockchain threats as surveyed in our work are given less attention. Further research on these organisational threats needs to be done to strengthen blockchain risk assessments and determine mitigating measures.

References

1. Bloomberg. bitcoin is having a civil war right as it enters a critical month. https://www.bloomberg.com/news/articles/2017-07-10/bitcoin-risks-splintering-as-civil-war-enters-critical-month.
2. Cambridge bitcoin electricity consumption index. https://www.cbeci.org/comparisons/.
3. Deloitte. blockchain risk management. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf.
4. enisa. ISO/IEC Standard 15408. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408.
5. ethernodes.org. https://www.ethernodes.org.
6. Marcella Atzori. Blockchain technology and decentralized governance: Is the state still necessary? *Available at SSRN 2709713*, 2015.
7. Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*, 2017.
8. Joram Borenstein. A risk-based view of why banks are experimenting with bitcoin and the blockchain. 2015. http://www.risktech-forum.com/opinion/a-risk-based-view-of-why-banks-are-experimenting-with-bitcoin-and-the-block.
9. Félix Brezo and Pablo G Bringas. Issues and risks associated with cryptocurrencies such as bitcoin. 2012.
10. Filip Caron. Blockchain: Identifying risk on the road to distributed ledgers. 2017. https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/blockchain-identifying-risk-on-the-road-to-distributed-ledgers.aspx?utm_referrer=.
11. Catherine Martin Christopher. The bridging model: Exploring the roles of trust and enforcement in banking, bitcoin, and the blockchain. *Nev. LJ*, 17:139, 2016.
12. Mauro Conti, E Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4):3416–3452, 2018.
13. Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10):71, 2016.
14. Alex De Vries. Bitcoin's growing energy problem. *Joule*, 2(5):801–805, 2018.
15. Claus Dierksmeier and Peter Seele. Cryptocurrencies and business ethics. *Journal of Business Ethics*, 152(1):1–14, 2018.
16. Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, and Mark Friedenbach. Strong federations: An interoperable blockchain solution to centralized third-party risks. *arXiv preprint arXiv:1612.05491*, 2016.
17. Food and agriculture organization of the united nations. E-agriculture in action: Blockchain for agriculture. 2019. https://www.ictworks.org/wp-content/uploads/2019/02/Blockchain-Agriculture.pdf.
18. Ivan Homoliak, Sarad Venugopalan, Qingze Hum, and Pawel Szalachowski. A security reference architecture for blockchains. *arXiv preprint arXiv:1904.06898*, 2019.
19. Tommy Koens and Erik Poll. Assessing interoperability solutions for distributed ledgers. *To appear in Pervasive and Mobile Computing, Elsevier*, 2019.

20. KPMG. Assessing blockchain risks. 2018. https://home.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/assessing-blockchain-risks.pdf.
21. Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6):1211–1220, 2017.
22. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. *Future Generation Computer Systems*, 2017.
23. Juho Lindman, Virpi Kristiina Tuunainen, and Matti Rossi. Opportunities and risks of blockchain technologies–a research agenda. 2017.
24. Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld, and Klaus Wehrle. A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. In *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer*, 2018.
25. WM Maurer and QI DuPont. Ledgers and law in the blockchain. 2015. https://www.weusecoins.com/assets/pdf/library/Ledgers%20and%20Law%20in%20the%20Blockchain.pdf.
26. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.
27. Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *International Conference on Financial Cryptography and Data Security*, pages 25–33. Springer, 2013.
28. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf.
29. Kay Noyen, Dirk Volland, Dominic Wörner, and Elgar Fleisch. When money learns to fly: Towards sensing as a service applications using bitcoin. *arXiv preprint arXiv:1409.5841*, 2014.
30. Karl J O'Dwyer and David Malone. Bitcoin mining and its energy footprint. 2014.
31. Harald Vranken. Sustainability of bitcoin and blockchains. *Current opinion in environmental sustainability*, 28:1–9, 2017.
32. Angela Walch. Open-source operational risk: Should public blockchains serve as financial market infrastructures? In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, pages 243–269. Elsevier, 2018.
33. Aaron Wright and Primavera De Filippi. Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*, 2015.
34. Dirk A Zetzsche, Ross P Buckley, and Douglas W Arner. The distributed liability of distributed ledgers: Legal risks of blockchain. *U. Ill. L. Rev.*, page 1361, 2018.