Avoiding Risky Designs When Using Blockchain Technologies in Cyber-Physical Systems

Nicholas Stifter*†, Matthias Eckhart*†, Bernhard Brenner*†, Edgar Weippl*†
*Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle, TU Wien, Vienna, Austria
†SBA Research, Vienna, Austria
firstname.lastname@sba-research.org

***Abstract*—Blockchain has been hailed as an emerging technology with the potential to cause significant impact in a variety of fields. One domain is an application in cyber-physical systems (CPSs), e.g., as a building block for the (Industrial) Internet of Things (IIoT) and Industry 4.0. In this regard, various use cases and designs have been proposed that seek to leverage the desirable properties blockchain technologies seem to offer. While many of the principles behind blockchain have actually been studied under the veil of Byzantine fault tolerance for decades, some approaches, such as relying on game-theoretic incentives and proof-of-work (PoW), are not yet fully understood. This knowledge gap can leave both practitioners and researchers in a difficult position regarding a possible application of such technologies, as it is often unclear what guarantees and characteristics a particular blockchain design actually achieves. This work-in-progress paper provides an overview of blockchain security research, outlines system designs that are likely to exhibit vulnerabilities, and provides examples of potentially insecure proposals in the field of CPSs that employ such designs.**

***Index Terms*—blockchain, security, cyber-physical systems**

I. Introduction

In the context of cyber-physical systems (CPSs), blockchain technologies seem particularly suited for areas where transparency, trust, and accountability is of utmost importance, such as supply chain management, energy management, or decentralized manufacturing. Many of the possible use cases in these domains are currently addressed either conceptually, or at an initial prototypical stage of implementation, as the necessary technological foundations and principles are still being established. The rapidly increasing body of research on existing blockchain protocols, as well as newly proposed designs and mechanisms, render it difficult to maintain oversight of these developments and incorporate new insights.

As a result, existing use cases and implementations of blockchain in CPSs may rely on incorrect assumptions that could compromise their security and correct operation. The consequences of vulnerable blockchain implementations are particularly severe in the context of CPSs, as compromised security can also lead to safety issues [1]. Although a considerable amount of literature has been published on possible applications of blockchain technologies within CPSs, previous research does not provide a critical evaluation of system attributes in existing concepts. Analyzing proposals in order to validate blockchain design decisions and their claimed security properties is fundamental for preventing technical debt, security issues, and the resulting safety implications. The paper at hand is aimed to address this gap. In particular, we provide an overview of security research on blockchain technologies and relate it to existing proposals that utilize blockchain in the context of CPSs, (I)IoT and Industry 4.0. Hereby, we show that beyond identifying appropriate use cases where blockchain could provide meaningful benefits, it is also essential to carefully consider the particular requirements and choose an adequate system model, as failure to do so may lead to insecure and vulnerable designs. The preliminary results presented in this work-in-progress paper provide an outlook on the development of a framework to support the decision-making process regarding the appropriate choice of blockchain technologies for particular use cases.

The financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development, and COMET K1, FFG - Austrian Research Promotion Agency is gratefully acknowledged.

II. Background

Blockchain technologies are the core enabling mechanism for decentralized cryptocurrencies such as Bitcoin [2]. Hereby, the necessity to trust a single third party to secure and update a distributed transaction ledger in order to prevent *double spending* of funds is avoided. The desirable characteristics blockchain-based distributed ledgers appear to offer has prompted various research fields and industries to explore possible applications of these technologies that extend well beyond peer-to-peer digital payments [3], [4].

It is important to note that many of the concepts, components, and goals behind blockchain have been the subject of study for decades [5]. In particular, the topic of *Byzantine fault tolerance* (BFT) is of interest, as it addresses how (distributed) systems can be designed to tolerate arbitrary failures or malicious behavior by a subset of its components. Many blockchain and cryptocurrency protocol designs, including Bitcoin, are targeted at an open, peer-to-peer setting with weak identities. In principle, in such a model anyone can participate in the consensus mechanism, observe the ledger's state, and issue transactions or state updates. This design principle is generally referred to as *permissionless*, whereas blockchains and distributed ledgers with a fixed set of consensus participants, stronger identities, and restrictions on who may issue state updates are called *permissioned* [6].

To achieve meaningful guarantees and BFT within a permissionless system model, trade-offs and additional assumptions are required compared to permissioned BFT protocols. Formal analyses regarding the differences and characteristics between blockchain and traditional BFT is a topic of ongoing research

978-1-7281-0303-7/19/$31.00 ©2019 IEEE

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:26:15 UTC from IEEE Xplore. Restrictions apply.

[7], [8]. By explicitly highlighting the ties between blockchain and BFT, we show its relevance to prior use cases in CPSs and (I)IoT where BFT may be advantageous.

III. Overview of Blockchain Security Research

A general overview of research perspectives and challenges for Bitcoin is given in [9]. The properties of the Bitcoin protocol, termed Nakamoto Consensus (NC), are first formally analyzed in [10] and an overview of related research is provided in [7], [8]. A discerning characteristic between NC and most BFT protocols is a lack of *consensus finality* in the former, i.e. only eventual consistency is achieved. This is a trade-off between *liveness* and *safety* of the underlying consensus [7]. Generally speaking, NC-style blockchains only achieve consistency over a *common prefix* of blocks with a probability that increases exponentially with newly mined blocks [10]. In practice, this means that the head of a blockchain can change, revert, or be conflicting and must first stabilize before being agreed upon. Failing to take this property into consideration may lead to incorrect system states, even within permissioned settings [11]. An analysis of parametrizations of public PoW blockchains and a framework to determine their security and performance is given in [12]. Sompolinsky and Zohar summarize and improve upon Bitcoin's security guarantees regarding *double spending attacks*, providing bounds for safely accepting transactions [13].

Missing consensus finality in NC also introduces the ability of block withholding attacks [14], [15] that adversely affect the *chain quality* [10]. Zhang and Preneel provide a comprehensive overview and analysis framework for security in PoW blockchains [16]. The game-theoretic components and modeling of player incentives in NC-style blockchains is still an open research question. Recently, Azouvi et al. provides a systematization of literature on the topic [17]. Bribing attacks constitute a particular aspect of rational players and player incentives [18]. Ullrich et al. discusses attacking reliable power grid operation through PoW cryptocurrencies [19]. Routing attacks have the potential to severely disrupt mining operations [20] and facilitate this scenario.

Depending on the particular application scenario or use case, blockchain technologies may not be an ideal solution. Wüst and Gervais [21] and Klein et. al. [22] provide frameworks for identifying appropriate use cases. Many permissionless and permissioned blockchain designs are novel and do not provide rigorous security and correctness analyses. Cachin and Vukolić [23] discusses a variety of blockchain consensus protocols and analyze their claimed characteristics.

a) Discussion: The above overview highlights that key characteristics of novel blockchain protocols are still the topic of discussion and their provided guarantees are not always clear. Many of the outlined attacks against NC-style PoW blockchains may also be adopted by an adversary in a permissioned PoW setting, once mining nodes are compromised. If a modest set of (permissioned) consensus participants is acceptable, relying on well-established BFT protocols currently remains a prudent approach, as the well researched, and often stronger, security guarantees and characteristics offer a clear advantage [24].

IV. Risk Indicators in Blockchain Characteristics

Based on our prior overview of blockchain security research, we highlight designs, system characteristics, and assumptions that are indicative of unproven or risky approaches. Systems that exhibit such properties are not necessarily vulnerable, however there exists considerably less research and experience, requiring additional diligence and careful protocol analysis to ensure correctness and security.

i. **Permissioned + Proof-of-Work:** An application of PoW in a permissioned setting is indicative of a less than ideal system configuration. The security guarantees of PoW are derived from an *honest computational majority* [2]. PoW can be readily outsourced to other hardware, and mechanisms to prevent this generally rely on game-theoretic incentives that do not apply in most permissioned systems. Further, PoW-based consensus generally only offers eventual consistency and not consensus finality.

ii. **Unproven Protocol Components and Primitives:** This includes consensus protocols and cryptographic algorithms that have not been formally analyzed and rigorously studied. Further, protocol compositions should also be re-evaluated as their security guarantees may change.

iii. **Additional Correctness Requirements:** Components or participants that are required to be correct at all times, beyond the defined thresholds for BFT, may present a single point of failure and can introduce further security risks. Different failure tolerance thresholds or permissible types of failures within the same system design also warrant closer inspection.

iv. **Permissioned + Dynamic Consensus Membership:** Achieving dynamic group membership in a Byzantine setting is a difficult problem [7]. Bitcoin and NC presents a particular solution in the permissionless setting, however general solutions for a permissioned environment with realistic system assumptions remain an open research question. Protocols that intend to achieve such guarantees should be carefully analyzed.

v. **Permissioned + Incentives:** The assumption of additional game-theoretic incentives, such as monetary reward structures, can be problematic as there is still considerably less security research on protocols employing these mechanisms [17]. Utilizing monetary incentives may furthermore introduce unwanted new attack surfaces through bribing and as a direct bounty for successful attacks.

vi. **Consistency Requirements + No Consensus Finality:** Special care needs to be taken if consensus safety guarantees are weakened, e.g., by a lack of finality. Unless confirmation times are carefully and appropriately chosen, various attacks become possible [13]. Proposals and use cases where this is the case should explicitly acknowledge and address the possible effects.

vii. **Sensitive Data in Transactions and Ledger:** If data contained within the ledger or any transactions may be

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:26:15 UTC from IEEE Xplore. Restrictions apply.

used by an adversary for attacks, the design should be closely examined for possible vulnerabilities.

V. Analysis of CPSs & (I)IoT Blockchain Use Cases

We present and analyze four proposed approaches of employing blockchain technologies in the context of CPSs and (I)IoT where the herein introduced risk indicators apply to aspects of the design. The analysis is not comprehensive and only serves to highlight that the presented guidelines are able to identify possible risk factors.

A. Securing SCADA Communication via the Blockchain

1) Approach: A blockchain-based scheme for securing SCADA communication using a *permissioned PoW blockchain* is presented in [25]. An optimization approach for choosing appropriate chain parametrizations is described to help ensure that the real-time requirements of control and monitoring functions are met by the underlying blockchain.

2) Possible Risk Factors: **i, v, vi;** An analysis of the presented system model highlights a possibly problematic assumption. It is indicated that the mining power remains constant for all designated mining entities. To prevent a miner from outsourcing its PoW, it is suggested to employ a technique presented by Eyal and Sirer [26], as well as utilizing a permissioned model where authorized miners are required to provide a valid signature for the PoW to be considered valid. However, such a deterrent against outsourcing is based on game-theoretic incentives that are not immediately applicable in the presented system model. It is hence likely possible that an adversary who has compromised a mining node can outsource the PoW and perform a variety of known attacks against NC-style blockchains, and possibly even achieve a computational majority within the network.

3) Possible Amendments: The reliance on PoW-based consensus should be replaced with a more established consensus mechanism that is specifically designed for the intended permissioned system model.

B. Collaborative Development of Power Electronic Devices

1) Approach: An approach for the collaborative development of power electronic devices using blockchain in the context of Industry 4.0 is presented in [27]. It is outlined how a *producer* may use a blockchain to present offers for the design and implementation of power electronic devices. Engineers that agree to the task and collaboratively solve the problem are automatically reimbursed using locked cryptocurrency units if the design is implemented and verified by all engineers. The possibility of blockchain forks is explicitly acknowledged, indicating a lack of consensus finality.

2) Possible Risk Factors: **iii, iv, vii;** The presented approach does not fully discuss and specify the necessary trust assumptions between all involved parties. Based on the available information, collaboration by malicious engineers could lead to defraudment of the producer by verifying an incorrect design and receiving subsequent payment. It is outlined that a producer may create new offers if previous ones were inadequate, necessitating some form of cancellation mechanism of old offers. It must be ensured that a producer cannot maliciously cancel or stall ongoing offers. In the presented design, data from engineers needs to be shared with other participants and may be stolen or copied by malicious parties that monitor transactions on the ledger. Further, an application of MultiChain within a permissioned setting may lead to undesirable characteristics of the underlying blockchain, as the protocol has not yet been rigorously analyzed [23].

3) Possible Amendments: The introduction of strong identities for all involved parties may help to disincentivize participant misbehavior. If a blockchain is used without finality, adequate stabilization time needs to be assured to avoid state reversions and forms of double-spending where the offer is reverted after the provided designs have already been published. It is unclear how collaboration can be readily fostered while preventing malicious parties from stealing or copying other designs. The introduction of a commit-reveal scheme may hamper such illicit front-running attempts.

C. Blockchain-based Protection Framework for Smart Meters

1) Approach: A distributed blockchain-based protection framework for smart meters to protect modern power systems against cyber attacks is proposed [28]. The approach builds on a reconfigured SCADA network that employs a PoW blockchain in a permissioned setting, together with a majority voting scheme to authenticate both mined blocks, as well as the sensor data that they include. This voting mechanism is intended as an additional countermeasure to prevent successful attacks unless a majority of the system is compromised.

2) Possible Risk Factors: **i, vi;** The presented scheme follows an interesting approach that can be considered a hybrid design between traditional BFT consensus protocols based on voting, and a PoW blockchain. However, in the design several essential aspects are not outlined. Without additional prevention mechanisms, a compromised miner may outsource its PoW, allowing it to perform censorship attacks on the data being committed by mining empty blocks. Further, it is unclear how consensus participants vote in case of blockchain forks and if tie-breaking mechanisms between competing blocks follow the longest chain rule such as Bitcoin [2] or employ some other mechanism. An adversary with sufficient mining power may either be able to revert an already committed state by mining another longer chain, or it may compromise liveness by logically partitioning the network and prevent a majority vote on blocks in case participants only vote for one of the competing blocks and reject all others as invalid. A more formal specification and analysis of the presented protocol seems necessary.

3) Amendments: Employing a well-studied, formally analyzed, BFT protocol with consensus finality that is executed by a clearly defined subset of nodes would largely address the outlined issues and also provide high data throughput.

D. Blockchain-based IIoT Architecture for Smart Factories

1) Approach: An IIoT architecture that leverages blockchain technologies and is targeted at enhancing

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:26:15 UTC from IEEE Xplore. Restrictions apply.

security and privacy in smart factories is presented in [29]. We hereby focus on the particular aspect of the proposal that employs blockchain technologies, namely the so called *management hub layer*. Hereby, the authors point out issues of employing PoW and accompanying incentive components of public blockchains and abandon them in favor of a permissioned setting. It is proposed to employ a form of PoW based on Statistical Process Control (SPC) or other comparison algorithms, however design details are left open.

2) Possible Risk Factors: **i, ii, vi;** In [29] the reliance on a PoW mechanism based on SPC or other comparison algorithms is suggested. However, a detailed protocol description and security analysis of the PoW design and subsequent blockchain construction is not provided. Based on the described properties and code examples, it is likely that finality is not guaranteed, as multiple *management hubs* appear to be able to broadcast blocks concurrently. Management hubs appear to act as a single trusted entity for sensors and devices connected to them from a *sensing layer* and may perform malicious actions such as selective censoring of data.

3) Amendments: A more traditional and well-studied BFT consensus algorithm such as PBFT (Practical Byzantine Fault Tolerance) should be employed, as it offers consensus finality and its security guarantees are well defined [30]. This approach is also acknowledged as a possible alternative to the proposed design by the authors themselves. The adversarial model may also need to be re-evaluated to ensure that a single management hub is unable to manipulate or censor data.

VI. Conclusion and Future Work

Within this work-in-progress paper we present current research for creating a decision framework by which risks and security issues within blockchain or distributed ledger designs, with a particular focus on CPSs and (I)IoT, can be identified. In contrast to prior art, our goal does not lie within identifying relevant use cases, but rather to identify whether a particular design or set of technologies presents a suitable choice for the given system model and whether the expected guarantees can actually be satisfied. Our analysis of existing proposals that exhibit design characteristics which we classify as risk indicators highlights their usefulness in identifying potential issues or vulnerabilities. In particular, we observe that the combination of permissioned blockchains and proof-of-work consensus is a risk prone design choice that could be readily avoided by relying on well-studied BFT consensus algorithms.

References

[1] B. Miller and D. Rowe, "A survey of scada and critical infrastructure incidents," in *Proc. of the 1st Annual Conference on Research in Information Technology*, ser. RIIT '12. ACM, 2012, pp. 51–56.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Dec 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2017, pp. 6153–6158.

[4] T. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. PP, pp. 1–1, 04 2019.

[5] A. Narayanan and J. Clark, "Bitcoin's academic pedigree," vol. 15, no. 4. New York, NY, USA: ACM, aug 2017, pp. 20:20–20:49.

[6] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," Apr 2015.

[7] N. Stifter, A. Judmayer, P. Schindler, A. Zamyatin, and E. Weippl, "Agreement with satoshi - on the formalization of nakamoto consensus," Cryptology ePrint Archive, Report 2018/400, 2018.

[8] J. Garay and A. Kiayias, "Sok: A consensus taxonomy in the blockchain era," Cryptology ePrint Archive, Report 2018/754, 2018.

[9] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *IEEE Symposium on Security and Privacy*, 2015.

[10] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology-EUROCRYPT 2015*. Springer, 2015, pp. 281–310.

[11] C. Natoli and V. Gramoli, "The blockchain anomaly," in *15th IEEE International Symposium on Network Computing and Applications*. IEEE, 2016, pp. 310–317.

[12] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. of the 2016 ACM SIGSAC*. ACM, 2016.

[13] Y. Sompolinsky and A. Zohar, "Bitcoin's security model revisited," 2016.

[14] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security*. Springer, 2014, pp. 436–454.

[15] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography and Data Security*, J. Grossklags and B. Preneel, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 515–532.

[16] R. Zhang and B. Preneel, "Lay down the common metrics: Evaluating proof-of-work consensus protocols' security," in *2019 IEEE Symposium on Security and Privacy*, 2019.

[17] S. Azouvi and A. Hicks, "Sok: Tools for game theoretic models of security for cryptocurrencies," *arXiv preprint arXiv:1905.08595*, 2019.

[18] P. McCorry, A. Hicks, and S. Meiklejohn, "Smart contracts for bribing miners," in *5th Workshop on Bitcoin and Blockchain Research, Financial Cryptography and Data Security 18 (FC). Springer*, 2018.

[19] J. Ullrich, N. Stifter, A. Judmayer, A. Dabrowski, and E. Weippl, "Proof-of-blackouts? how proof-of-work cryptocurrencies could affect power grids," in *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 2018, pp. 184–203.

[20] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 375–392.

[21] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018.

[22] S. Klein and W. Prinz, "A use case identification framework and use case canvas for identifying and exploring relevant blockchain opportunities," in *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.

[23] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," arXiv:1707.01873, 2017, accessed:2017-09-26.

[24] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *International Workshop on Open Problems in Network Security*. Springer, 2015, pp. 112–125.

[25] K. Koumidis, P. Kolios, and C. Panayiotou, "Optimizing blockchain for data integrity in cyber physical systems," 01 2018, pp. 73–80.

[26] I. Eyal and E. G. Sirer, "How to Disincentivize Large Bitcoin Mining Pools," Available: (http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools), [Accessed: 12-July-2019].

[27] Y. Yan, B. Duan, Y. Zhong, and X. Qu, "Blockchain technology in the internet plus: The collaborative development of power electronic devices," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2017, pp. 922–927.

[28] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[29] J. Wan, J. Li, M. Imran, D. Li, and F. e-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[30] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999, pp. 173–186.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:26:15 UTC from IEEE Xplore. Restrictions apply.