What is Meant by *Permissionless* Blockchains?

Nicholas Stifter*†, Aljosha Judmayer†*, Philipp Schindler*†, Walid Fdhila*, and Edgar Weippl †*
*SBA Research, Vienna, Austria
(firstletterfirstname)(lastname)@sba-research.org
†University of Vienna, Vienna, Austria

***Abstract*—The term *permissionless* has established itself within the context of blockchain and distributed ledger research to characterize protocols and systems that exhibit similar properties to Bitcoin. However, the notion of what is meant by permissionlessness is often vague or left implicit within the various literature, rendering it imprecise and hard to compare. We hereby shed light onto this topic by revising research that either incorporates or defines the term *permissionless* and systematically expose the properties and characteristics that its utilization intends to capture. Based on this review, we highlight current shortcomings and blind spots within the available definitions. In particular, the ability to freely perform transactions between users is often not adequately incorporated and different actor roles are left unspecified. Furthermore, the topics of privacy and governance appear to be largely overlooked.**

I. Introduction

The use of the term *"permissionless"* in the context of blockchain and distributed ledger research first emerged in scientific literature around 2015 (e.g.[1], [2]) and has since steadily gained in popularity, finding its way into the titles of top-tier publications.[3] Despite this relatively quick success in adoption, there currently exists no established definition of "permissionless" and the desirable properties and characteristics that a permissionless system should encompass. Furthermore, many publications utilize the term without providing or pointing toward a definition, leading to possible confusion about its intended meaning and hampering overall comparability. This apparent lack of a common terminology is surprising, given that permissionlessness is often attributed as the distinguishing characteristic of Bitcoin and similar cryptocurrency systems.

In this paper we seek to render the notion of permissionlessness more explicit. Hereby, we first systematically analyze its utilization and definitions in prior research and then extract and categorize the various properties and characteristics that the term intends to encompass. Through an iterative process, we establish a classification framework for definitions of the term permissionless, and apply this framework to a well defined set of literature consisting of publications from 8 of the top ranked security and cryptology conferences that are among the premiere venues for presenting blockchain and distributed ledger research. The resulting categorization includes both prevalent and unique definition elements which we were able to extract from the various literature. We subsequently challenge current practices and beliefs regarding the classification of permissionless blockchains and distributed ledger technologies (DLTs), and show that there exist both shortcomings, as well as possible combinations of properties within the design space where current definitions prove inadequate or incapable of capturing important nuances. A particularly interesting observation from our analysis of current definitions is an underrepresentation, or lack of consideration, regarding the ability for regular users to freely perform transactions with each other as part of the defining characteristics of a permissionless system. Surprisingly, this aspect *is* partially addressed by formal modeling approaches of Nakamoto-style blockchains and their consensus mechanisms [4], [5], [6] which contain a liveness property for transactions that guarantees their eventual inclusion as a desirable characteristic, yet no such requirement can be found in more general definitions.

Summarizing, this paper offers the following contributions:

- A systematic exposition of the term *permissionless* and its definitions in various peer reviewed literature through a classification framework we derive.
- Novel insights and arguments that challenge the current views what may be considered a permissionless system.
- Suggestions for possible augmentations to current definitions to address shortcomings in their ability to capture permissionlessness.
- Identification of future research directions and challenges

II. The Meaning of "Permissionless" in Current Research

The scope of this work is to analyze and categorize the current utilization of the term 'permissionless' in the context of blockchain and distributed ledger research that is focused on the underlying technology. In the following, we first outline the methodology consisting of 5 steps on which our analysis is based. We then present our results, including both prevalent and unique definition elements which we were able to extract. We point out that the notion of permissionlessness is often conflated with aspects of decentralization, the latter having already been systematically studied, e.g., in regard to privacy [7]. However, while there is a clear overlap in the aspects that these terms address, the term "permissionless" is much more intimately linked to Bitcoin, cryptocurrencies, and their distributed consensus protocols. The fact that it is now widely used within this field of research to classify blockchains and DLTs clearly warrants a more in-depth discussion. We envision to expand upon this analysis by also including the definition of *permissioned* systems and other properties that are used to describe different types of blockchain and DLT systems in future work.

A. Analysis Method

The methodology consists of the following five steps:

1) Step 1): In the first Step, we cast a wide net to establish a broad repository composed of peer-reviewed publications, technical reports, and grey literature on the subject of blockchain and DLTs that include the term "permissionless" in the text body. For this, we turn to repositories dedicated to blockchain research, [1] as well as the top ranked 300 results using the search term *blockchain OR bitcoin OR cryptocurrency OR "distributed ledger"* in both, google scholar and DBLP.[2] Our data collection was hereby assisted by utilizing Zotero[3] to help scrape search results and automate the gathering of corresponding pdf files, where publicly available. These manuscript files were then parsed using `pdfgrep` to locate literature where the word "permissionless" is used within the text body. This first selection process resulted in well over 600 potential matches, however we point out that this includes various duplicate or closely related entries due to different manuscript versions.

2) Step 2): Manual filtering of the repository from Step 1 was performed to identify works that provide either more detailed definitions, or address the topic from unique angles. Works were targeted that either highlight the most commonly encountered definitions and properties or contain unique or uncommon approaches that set themselves apart. We outline that the purpose of this first round of analysis is the discovery of a wide range of different definition approaches to ensure that enough categories are established when specifying the classification framework and avoid having to extend or add categories during further analyses. Hence, we argue that such a loosely defined manual selection is acceptable in this context. This selection yielded $n = 68$ manuscripts from which we extracted both the concrete definitions, as well text passages covering the topic, to derive a set of keywords for defining elements of, as well as important concepts related to, the presented definition.

3) Step 3): We derive an initial classification framework prototype for definitions of "permissionless" through an iterative process, based on the keywords and concepts generated in the previous step. Subsequently, we test the ability and effectiveness of our framework to capture meaningful aspects and dimensions related to "permissionless" definitions by analyzing a total of $n = 28$ papers selected from Step 2.

4) Step 4): Equipped with this novel classification framework, we set out to analyze a more precisely defined set of literature by considering publications from 8 of the top ranked security and cryptology conferences that are among the premiere venues for presenting blockchain and distributed ledger research. Available conference papers were collected from within the last 6 years (Jan. 2014 to Aug. 2020). The time range was specifically chosen as the earliest works utilizing *permissionless* that we were able to identify correspond to the year 2015. Our process for filtering relevant publications containing "permissionless" from this collection follows analogous to Step 1 and yields a total of $n = 55$ works, namely 17 from the ACM SIGSAC Conference on Computer and Communications Security (CCS), 8 from the IEEE Symposium on Security and Privacy (SP), 3 from the USENIX Security Symposium (USENIX), 11 from the Annual Network and Distributed System Security Symposium (NDSS), 2 from the Annual International Cryptology Conference (CRYPTO), 4 from the Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), 8 from Financial Cryptography and Data Security (FC), and 2 from the International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt).

5) Step 5): Finally, the classification framework derived in Step 3 is applied to the relevant literature from Step 4 and the results summarized in Subsection II-B. See Tables 0a and 0a in the Appendix for a listing of the aforementioned literature and associated categorization artifacts.

B. Categorizing Definitions of "Permissionless" Related to Blockchain and DLT Research

We first outline the components of the classification framework used to compare and categorize different definitions that were iteratively derived. The following elements and properties intend to capture core aspects and different focal points in available definitions of the term permissionless. We introduce the following 6 main categories to which we ascribe different elements of the definition. The assignment to main categories is not strictly hierarchical, meaning that different categories may share definition elements. As an example, if a definition of permissionless contains the (hypothetical) statement "anyone can verify transactions and mine blocks to earn fees" it is categorized both under *ledger interaction* as well as *trust*.

- *Description.* In this category we place definitions and descriptions of what is meant by "permissionless" and concrete examples given of systems or designs that can be permissionless, e.g., Bitcoin, cryptocurrencies, or proof-of-stake.
- *Actors.* Here we categorize definition elements pertaining to actors and their identities. For instance, the ability to *join and leave*, if the term *Sybil* is mentioned, or if there are different actor roles, e.g., *miners, users, anyone*.
- *Ledger Interaction.* This category covers how definitions address any interaction with the underlying blockchain or ledger and its data and includes items such as *validation* and *data availability*. We propose to use the following sub-categories with different actor roles akin to file-system permissions:
  - Read: the ability to *read* previous ledger states, transactions and data.
  - Write: the ability to *write* to, and *update*, the ledger state.
  - Execute: the ability to perform *transactions* is often described as a write operation. We modify this view and consider a transaction to represent a computation that may also read or write.
- *Trust.* In this category we collect definition elements that relate to trust, such as *(no)authorization*, as well as game-theoretic aspects such as *incentives* or *rational* behavior.

[1] cf. blockchainbib https://allquantor.at/blockchainbib/, cabra https://cdecker.github.io/btcresearch/ and decrypto https://github.com/decrypto-org/blockchain-papers

[2] cf. google scholar https://scholar.google.com, DBLP https://dblp.org

[3] cf. Zotero https://www.zotero.org

- *Privacy.* If elements of the definition explicitly touch on the topic of privacy they are placed into this category.
- *Other.* The final category is used as an overflow bucket for unanticipated categories or unique elements. It captures both definition elements we identified in Step 3) as relevant, yet not common enough to warrant a whole category, as well as any other interesting or noteworthy items. After our analysis the following items ended up being included: *governance*, *network layer* and *consensus*.

In order to aid in explorative analysis, we visualize common composition elements that were used in the context of the term permissionless and its definitions through a co-occurrence graph of the results obtained through our classification framework, shown in Figure 1. To improve readability, we omit any data elements from the graph that only have a single occurrence and *Description* was split into *definition* and *examples*. Nodes represent both categories and their contained and processed elements. The complete list of composition elements that serves as the basis for this visualization is provided in the Appendix in Tables 0a and 0a.

III. Are Current Definitions Adequate?

We hereby iterate over the results from analyzing publications from 8 top ranked conference venues that contain the term "permissionless" within its text body or title using our classification framework and discuss their relationship in regard to current definitions and descriptions of permissionless. Of the reviewed 55 publications that contain the term, only 20 (≈36%) provide a more concrete definition (6 in CCS, 4 in SP, 1 in USENIX, 4 in NDSS, 1 in CRYPTO, 3 in Eurocrypt, 0 in FC, 1 in Asiacrypt).

A. Discussion of Classification Results based on Categories

1) Descriptions: We observe that while $\approx 64\%(35)$ of the considered works provide practical examples of permissionless systems only $\approx 36\%(20)$ offer concrete definitions. Overall $\approx 51\%(28)$ consider Bitcoin to be such an example and $\approx 36\%(20)$ include other systems and approaches such as Ethereum, proof-of-stake (PoS), or variants of Byzantine fault tolerance (BFT) protocols. While we believe that providing concrete examples for permissionless systems can be helpful, their concrete design considerations are often not homogeneous enough to make the properties of what is meant by "permissionless" clear, and their designs may also be subject to change, such as the intended transition from proof-of-work to PoS in Ethereum.

2) Actors: Here, $\approx 31\%(17)$ of papers mention the ability to *join and leave* as an element of permissionlessness, while those that also provide a concrete definition include it 70%(14) of the time. The closely related term *open* appears in $\approx 15\%(8)$ of all works in this context. Actor models are currently not made very explicit and usually encompass a single actor category that is responsible for all interactions, which is sometimes described using terms such as *anyone* $\approx 11\%(6)$. Out of the analyzed works $\approx 4\%(2)$ of descriptions are phrased such that they suggest the existence of more than one actor role within the system. We find this surprising, given that more than half of the papers rely on Bitcoin as an example, which defines different actor roles, namely *full network nodes* and *simplified payment verification (SPV)*, whose abilities and underlying trust assumptions differ (see Appendix A). The utilization of SPV wallets is nowadays widespread in most cryptocurrencies, yet the definitions of "permissionless" currently do not adequately capture this difference in user interaction, raising the question if the intended meaning of permissionless extends to both roles. In light of research targeted at both attacking and improving the security of such light client implementations [8], we believe it is important for definitions of permissionless to more explicitly capture and consider all of the different possible actor models within such systems.

Our argument regarding different actor models is further strengthened by research on cryptocurrency mining and its decentralization[9], [10], suggesting a stronger distinction between the actor roles for reaching agreement and writing to the ledger, and those actors that merely wish to execute transactions. Indeed, at the current mining difficulty level of the Bitcoin network (01.01.2021), even if dedicated hardware capable of performing 100 TerraHashes per second is employed, a participant would in expectation be able to partake in Bitcoin's consensus mechanism by successfully solo-mining a block roughly once every 25 years.[4] Users may hence pool together to form *mining pools*, however while there exist proposals for pooled mining where individual participants could in principle influence the pool's block proposal [11], or render it more trustless through smart contracts [10], the current predominant mode of operation delegates all trust and permissions to the mining pool operators, whose actions and behavior may not always be transparent and accountable [12], [13].

3) Ledger Interaction: Our results show that $\approx 29\%(16)$ of the total, and 40%(8) of papers with concrete definitions, include aspects from this category in their descriptions. Based on our analysis, as well as the larger body of literature we reviewed to derive our framework, we believe that many current definitions of "permissionless" contain a blind spot within the *execute* sub-category that is not immediately apparent. Specifically, we find that the intended ability for users to meaningfully interact with the system by performing transactions between each other is not adequately captured. We derive this intended property on the one hand from the descriptions within the Bitcoin whitepaper [14], and on the other hand from the fact that a majority of works use it as an example of a permissionless system (see Appendix A). Interestingly, many works that formally analyze Nakamoto consensus (e.g. [4], [5], [6]) actually touch on this topic by defining a *liveness* property which guarantees that transactions from honest participants are included in the common prefix of the ledger within some upper time bound Δ. It would seem appropriate to also adopt such a *transaction liveness* property to definitions of "permissionless". However, we note that to achieve such transaction liveness in practice either the size of blocks must be unbounded, or the rate at which transactions can be spawned limited, both of which raise

[4]Based on the mining difficulty of 18599593048299 and a device capapble of 100TH/s the expected time for finding a Bitcoin block is $18599593048299 * 2^{32}/(10^{14} * 60 * 60 * 24) = 9245.907854323283\, hours \approx 25\, years$.

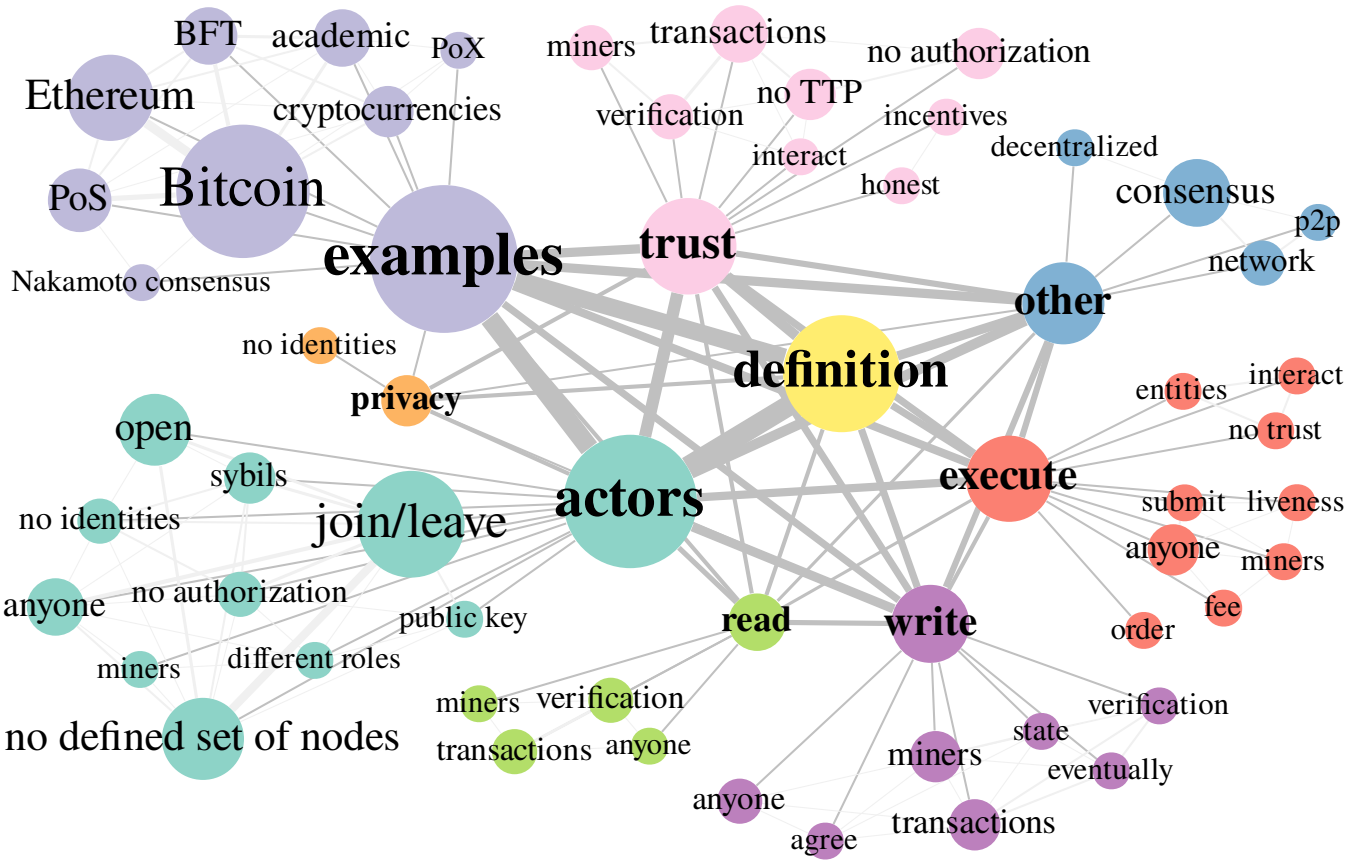

Fig. 1. Results of proposed categorization framework for descriptions and definitions related to the term "permissionless" gathered from 8 top ranked security conferences, visualized as a co-occurence graph with single-count elements excluded.

new and interesting questions how to meaningfully define permissionlessness in the context of transactions. A closely related problem are possible attacks on transaction ordering or exclusion by consensus participants [15], [16], [17], which follows a long line of research on *bribing attacks* [18] and may also negatively affect users. It is still unclear how definitions of permissionlessness should meaningfully capture these game-theoretic aspects.

4) Trust: Within our trust category commonly found description elements address miners, transactions, mention of no trusted third parties (TTPs), verification and incentives. Our analysis hence highlights the seemingly obvious, namely that definition elements of the notion of permissionless which relate to trust would also contain references to transactions, the miners that process them, and their incentives. It is interesting to note that while several definitions of "permissionless" acknowledge the actor role of miners, most specify that every participant actually is a miner and do not make any further distinctions.

5) Privacy: A surprising result from our analysis is an apparent lack of definition elements that more concretely include privacy aspects in their descriptions of permissionless. In total only four works, which all provide definitions of permissionless, contain elements we place into the privacy category, meaning $\approx 7\%(4)$ of all and respectively $\approx 18\%(4)$ of works with definitions cover this angle. The elements leading to their categorization mostly relate to anonymity or the lack of pre-established identities. In regard to privacy and permissionlessness, we are inspired [19] to the following interesting line of thought: By providing indistinguishably and privacy through cryptographic techniques, such as zero-knowledge protocols, strong notions of permissionlessness may not only be achievable in privacy-oriented cryptocurrencies [20], [21] but may also apply to users of systems that are controlled by trusted third parties. In such cases operators may only be able to indiscriminately deny their service to all interacting parties or none. A deeper understanding of the interplay between privacy preserving techniques and their potential ability to affect the permissionlessness of a system is hence also of relevance and could lead to more refined definitions.

6) Other: One of the main aspects that was not adequately covered through the framework's categories is the topic of *consensus*. Nakamoto consensus is arguably one of Bitcoin's core innovations and scientific contributions [22], [23], which is reflected by the many works that either seek to analyze and formalize [4], [5], [6] or build and extend upon its concepts [24]. We believe that for future analysis this should be used as a full category in the categorization framework.

Another highly relevant, yet largely overlooked aspect of permissionlessness is the topic of *governance*, which is not meaningfully touched by any of the herein considered definitions. Capturing the ability to modify protocol rules

and functionalities, thereby possibly changing core elements that define if it can be considered permissionless, present an interesting challenge when defining permissionlessness. Again, this issue strongly relates to a lack of more concise actor roles. However, on-chain programmatic approaches to governance [25], [26], [27], both on the protocol level or in the form of smart contracts, present an interesting outlook how such aspects could be more clearly defined and captured within future definitions of permissionless.

B. Limitations of Analysis

We highlight several limitations and shortcomings that are inherent to our chosen approach. The establishment of our classification framework and its categories was exploratory in nature and may not have captured all relevant aspects. To combat this, we intentionally selected a wider body of literature as the basis for its creation. Given this large volume of considered literature, it was infeasible to capture, in-depth, the intended meaning of the term "permissionless" if it was not clearly outlined within its text. Further, if a publication exclusively utilized another descriptor, such as "decentralized" or "open" it was not considered by our analysis. Another aspect to consider is that some papers primarily target a specific topic related to permissionlessness, such as the previously mentioned topic of consensus, and may hence intentionally not cover all aspects.

IV. Future Outlook and Conclusion

We have raised the question whether current definitions of "permissionless" are adequate and through our analysis and discussion come to the conclusion that several aspects either fall short in their intended meaning, or do not capture vital elements. By shining light on how the term is currently used, and exposing possible shortcomings and blind spots, a broader community discussion the subject matter may be sparked. Finding a more concise definition would not only benefit comparability between literature, but could also focus attention on aspects, such as enabling any user of a "permissionless" system to freely transact without being exposed to possible censorship- and transaction-ordering attacks from miners, all the while respecting her privacy.

Beyond this immediate goal also lie several interesting future research challenges. The ability to implement higher layer applications and interoperability measures [28] on top of distributed ledgers raises the question how they may affect the current permissions of actors within such systems. Similarly, smart contract capable platforms allow users to augment a system's properties such as its privacy [29]. Finally, our analysis has shown that the various properties intended to be captured by the term "permissionless" do not readily lend themselves for a Boolean answer, raising legitimate doubts to its usefulness as a descriptor.

Acknowledgment

This material is based upon work partially supported by (1) the Christian-Doppler-Laboratory for Security and Quality Improvement in the Production System Lifecycle; The financial support by the Austrian Federal Ministry for Digital and Economic Affairs, the Nation Foundation for Research, Technology and Development and University of Vienna, Faculty of Computer Science, Security & Privacy Group is gratefully acknowledged; (2) SBA Research; the competence center SBA Research (SBA-K1) funded within the framework of COMET Competence Centers for Excellent Technologies by BMVIT, BMDW, and the federal state of Vienna, managed by the FFG; (3) the FFG Bridge 1 project 864738 PR4DLT. (4) the FFG ICT of the Future project 874019 dIdentity & dApps. (5) the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078 (FeatureCloud). We would also like to thank our anonymous reviewers for their valuable feedback and suggestions.

References

[1] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *International Workshop on Open Problems in Network Security*. Springer, pp. 112–125. [Online]. Available: http://vukolic.com/iNetSec_2015.pdf

[2] T. Swanson, *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*. [Online]. Available: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[3] D. Deuber, B. Magri, and S. A. K. Thyagarajan, "Redactable blockchain in the permissionless setting," published: arXiv:1901.03206. [Online]. Available: https://arxiv.org/pdf/1901.03206.pdf

[4] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology-EUROCRYPT 2015*. Springer, pp. 281–310. [Online]. Available: http://courses.cs.washington.edu/courses/cse454/15wi/papers/bitcoin-765.pdf

[5] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, pp. 643–673. [Online]. Available: https://eprint.iacr.org/2016/454.pdf

[6] C. Badertscher, U. Maurer, D. Tschudi, and V. Zikas, *Bitcoin as a Transaction Ledger: A Composable Treatment*, published: Cryptology ePrint Archive, Report 2017/149. [Online]. Available: https://eprint.iacr.org/2017/149.pdf

[7] C. Troncoso, G. Danezis, M. Isaakidis, and H. Halpin, "Systematizing decentralization and privacy: Lessons from 15 years of research and deployments," in *Proceedings on Privacy Enhancing Technologies*, pp. 307–329. [Online]. Available: https://petsymposium.org/2017/papers/issue4/paper87-2017-4-source.pdf

[8] S. Paavolainen and C. Carr, "Security properties of light clients on the ethereum blockchain," *IEEE Access*, vol. 8, pp. 124 339–124 358, 2020.

[9] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, "Decentralization in bitcoin and ethereum networks," in *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer*. [Online]. Available: http://fc18.ifca.ai/preproceedings/75.pdf

[10] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "SmartPool: Practical decentralized pooled mining." [Online]. Available: https://eprint.iacr.org/2017/019

[11] Bitcoin Wiki. (2019) getblocktemplate. [Online]. Available: https://web.archive.org/web/20201130222835/https://en.bitcoin.it/wiki/Getblocktemplate

[12] A. Judmayer, A. Zamyatin, N. Stifter, A. G. Voyiatzis, and E. Weippl, "Merged mining: Curse or cure?" in *CBT'17: Proceedings of the International Workshop on Cryptocurrencies and Blockchain Technology*. [Online]. Available: https://eprint.iacr.org/2017/791.pdf

[13] M. Romiti, A. Judmayer, A. Zamyatin, and B. Haslhofer, "A deep dive into bitcoin mining pools: An empirical analysis of mining shares," in *The 2019 Workshop on the Economics of Information Security*. [Online]. Available: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_30.pdf

[14] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, published: arXiv preprint arXiv:1904.05234. [Online]. Available: https://arxiv.org/pdf/1904.05234.pdf

[16] S. Eskandari, S. Moosavi, and J. Clark, "SoK: Transparent dishonesty: front-running attacks on blockchain," in *arXiv preprint arXiv:1902.05164*. [Online]. Available: https://arxiv.org/pdf/1902.05164.pdf

[17] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels, "Order-fairness for byzantine consensus." [Online]. Available: https://eprint.iacr.org/2020/269

[18] A. Judmayer, N. Stifter, A. Zamyatin, I. Tsabary, I. Eyal, P. Gaži, S. Meiklejohn, and E. Weippl, *Pay-To-Win: Incentive Attacks on Proof-of-Work Cryptocurrencies*, published: Cryptology ePrint Archive, Report 2019/775. [Online]. Available: https://eprint.iacr.org/2019/775.pdf

[19] D. C. Sánchez, "Zero-knowledge proof-of-identity: Sybil-resistant, anonymous authentication on permissionless blockchains and incentive compatible, strictly dominant cryptocurrencies," *arXiv preprint arXiv:1905.09093*, 2019.

[20] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*. IEEE, pp. 459–474.

[21] S. Noether, "Ring signature confidential transactions for monero." [Online]. Available: https://eprint.iacr.org/2015/1098

[22] 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*. [Online]. Available: http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf

[23] N. Stifter, A. Judmayer, P. Schindler, A. Zamyatin, and E. Weippl, *Agreement with Satoshi - On the Formalization of Nakamoto Consensus*, published: Cryptology ePrint Archive, Report 2018/400. [Online]. Available: https://eprint.iacr.org/2018/400.pdf

[24] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, *Consensus in the Age of Blockchains*, published: arXiv:1711.03936. [Online]. Available: https://arxiv.org/pdf/1711.03936.pdf

[25] L. Goodman, "Tezos—a self-amending crypto-ledger white paper," 2014. [Online]. Available: https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf

[26] A. Norta, "Designing a smart-contract application layer for transacting decentralized autonomous organizations," in *International Conference on Advances in Computing and Data Sciences*. Springer, 2016, pp. 595–604.

[27] W. Reijers, I. Wuisman, M. Mannan, P. De Filippi, C. Wray, V. Rae-Looi, A. C. Vélez, and L. Orgad, "Now the code runs itself: On-chain and off-chain governance of blockchain technologies," *Topoi*, pp. 1–11, 2018.

[28] P. McCorry and A. Gervais, "SoK: Layer-two blockchain protocols," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers*, vol. 12059. Springer Nature, p. 201. [Online]. Available: http://fc20.ifca.ai/preproceedings/150.pdf

[29] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards privacy in a smart contract world." [Online]. Available: https://eprint.iacr.org/2019/191

[30] 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 (SP). IEEE*. [Online]. Available: https://www.esat.kuleuven.be/cosic/publications/article-3005.pdf

[31] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt, "Xclaim: Trustless, interoperable, cryptocurrency-backed assets," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 193–210.

[32] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 583–598.

[33] A. Tomescu and S. Devadas, "Catena: Efficient non-equivocation via bitcoin," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 393–409.

[34] H. Yu, I. Nikolić, R. Hou, and P. Saxena, "Ohie: Blockchain scaling made simple," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 90–105.

[35] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A stealthier partitioning attack against bitcoin peer-to-peer network," in *To appear in Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P)*. [Online]. Available: https://erebus-attack.comp.nus.edu.sg/erebus-attack.pdf

[36] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, "HyperService: Interoperability and programmability across heterogeneous blockchains." [Online]. Available: https://eprint.iacr.org/2020/578

[37] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Prism: Deconstructing the blockchain to approach physical limits," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 585–602.

[38] C. Egger, P. Moreno-Sanchez, and M. Maffei, "Atomic multi-channel updates with constant collateral in bitcoin-compatible payment-channel networks." [Online]. Available: https://eprint.iacr.org/2019/583

[39] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-time cryptocurrency exchange using trusted hardware," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1521–1538.

[40] I. Tsabary and I. Eyal, "The gap game," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 713–728. [Online]. Available: https://arxiv.org/pdf/1805.05288.pdf

[41] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Bünzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 67–82.

[42] M. Bartoletti and R. Zunino, "BitML: A calculus for bitcoin smart contracts." [Online]. Available: https://eprint.iacr.org/2018/122

[43] M. Zamani, M. Movahedi, and M. Raykova, *RapidChain: A Fast Blockchain Protocol via Full Sharding*, published: Cryptology ePrint Archive, Report 2018/460. [Online]. Available: https://eprint.iacr.org/2018/460.pdf

[44] R. Khalil and A. Gervais, *Revive: Rebalancing Off-Blockchain Payment Networks*, published: Cryptology ePrint Archive, Report 2017/823. [Online]. Available: http://eprint.iacr.org/2017/823.pdf

[45] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, *Concurrency and Privacy with Payment-Channel Networks*. [Online]. Available: https://www.cs.purdue.edu/homes/pmorenos/public/paychannels.pdf

[46] J. Camenisch, M. Drijvers, and M. Dubovitskaya, "Practical UC-secure delegatable credentials with attributes and their application to blockchain," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. Association for Computing Machinery, pp. 683–699, event-place: Dallas, Texas, USA. [Online]. Available: https://doi.org/10.1145/3133956.3134025

[47] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 17–30. [Online]. Available: https://www.comp.nus.edu.sg/prateeks/papers/Elastico.pdf

[48] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of BFT protocols," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 31–42. [Online]. Available: https://eprint.iacr.org/2016/199.pdf

[49] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *23rd ACM Conference on Computer and Communications Security (ACM CCS 2016)*. [Online]. Available: https://eprint.iacr.org/2016/633.pdf

[50] G. Chen, Y. Zhang, and T.-H. Lai, "OPERA: Open remote attestation for intel's secure enclaves," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2317–2331.

[51] L. Kiffer, R. Rajaraman, and A. Shelat, "A better method to analyze blockchain consistency," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 729–744.

[52] A. Tomescu, V. Bhupatiraju, D. Papadopoulos, C. Papamanthou, N. Triandopoulos, and S. Devadas, "Transparency logs via append-only authenticated dictionaries," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1299–1316.

[53] S. Matetic, K. Wüst, M. Schneider, K. Kostiainen, G. Karame, and S. Capkun, "${$bite$}$: Bitcoin lightweight client privacy using trusted execution," in *28th ${$USENIX$}$ Security Symposium (${$USENIX$}$ Security 19)*, pp. 783–800.

[54] P. Szalachowski, D. Reijsbergen, I. Homoliak, and S. Sun, "StrongChain: Transparent and collaborative proof-of-work consensus." [Online]. Available: http://arxiv.org/abs/1905.09655

[55] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. v. Renesse, *REM: Resource-Efficient Mining for Blockchains*, publication Title: Cryptology ePrint Archive, Report 2017/179. [Online]. Available: http://eprint.iacr.org/2017/179.pdf

[56] V. Mavroudis, K. Wüst, A. Dhar, K. Kostiainen, and S. Capkun, *Snappy: Fast On-chain Payments with Practical Collaterals*, _eprint: arXiv:2001.01278. [Online]. Available: https://arxiv.org/pdf/2001.01278.pdf

[57] S. Das, V. J. Ribeiro, and A. Anand, "YODA: Enabling computationally intensive contracts on blockchains with byzantine and selfish nodes," in *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-4_Das_paper.pdf

[58] D. Derler, K. Samelin, D. Slamanig, and C. Striecks, "Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based." [Online]. Available: https://eprint.iacr.org/2019/406

[59] D. Leung, A. Suhl, Y. Gilad, and N. Zeldovich, "Vault: Fast bootstrapping for the algorand cryptocurrency," in *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_09-2_Leung_paper.pdf

[60] A. Sonnino, M. Al-Bassam, S. Bano, S. Meiklejohn, and G. Danezis, "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers," in *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_06A-1_Sonnino_paper.pdf

[61] G. Malavolta, P. Moreno-Sanchez, A. Kate, and M. Maffei, "SilentWhispers: Enforcing security and privacy in decentralized credit networks," in *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*. The Internet Society. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss201701-5MalavoltaPaper.pdf

[62] S. Kalra, S. Goel, M. Dhawan, and S. Sharma, "ZEUS: Analyzing safety of smart contracts," in *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. The Internet Society. [Online]. Available: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-1_Kalra_paper.pdf

[63] D. Perez and B. Livshits, "Broken metre: Attacking resource metering in EVM." [Online]. Available: http://arxiv.org/abs/1909.07220

[64] P. Ekparinya, V. Gramoli, and G. Jourjon, "The attack of the clones against proof-of-authority," in *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24082-paper.pdf

[65] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability," in *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_09-4_Malavolta_paper.pdf

[66] H. Ritzdorf, K. Wüst, A. Gervais, G. Felley, and S. Capkun, "TLS-n: Non-repudiation over TLS enablign ubiquitous content signing," in *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. The Internet Society. [Online]. Available: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-4_Ritzdorf_paper.pdf

[67] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels, "Order-fairness for byzantine consensus," in *Advances in Cryptology – CRYPTO 2020*, ser. Lecture Notes in Computer Science, D. Micciancio and T. Ristenpart, Eds. Springer International Publishing, pp. 451–480.

[68] S. Dziembowski, L. Eckey, S. Faust, J. Hesse, and K. Hostáková, "Multi-party virtual state channels." [Online]. Available: https://eprint.iacr.org/2019/571

[69] R. Pass and E. Shi, "Thunderella: Blockchains with optimistic instant confirmation," in *Advances in Cryptology – EUROCRYPT 2018*, ser. Lecture Notes in Computer Science, J. B. Nielsen and V. Rijmen, Eds. Springer International Publishing, pp. 3–33.

[70] J. Garay, A. Kiayias, R. M. Ostrovsky, G. Panagiotakos, and V. Zikas, "Resource-restricted cryptography: Revisiting MPC bounds in the proof-of-work era," in *Advances in Cryptology – EUROCRYPT 2020*, ser. Lecture Notes in Computer Science, A. Canteaut and Y. Ishai, Eds. Springer International Publishing, pp. 129–158.

[71] K. A. Negy, P. R. Rizun, and E. G. Sirer, "Selfish mining re-examined," in *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10-14, 2020 Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Bonneau and N. Heninger, Eds., vol. 12059. Springer, pp. 61–78.

[72] R. Stütz, P. Gazi, B. Haslhofer, and J. Illum, "Stake shift in major cryptocurrencies: An empirical study," in *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10-14, 2020 Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Bonneau and N. Heninger, Eds., vol. 12059. Springer, pp. 97–113. [Online]. Available: https://doi.org/10.1007/978-3-030-51280-4_7

[73] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "SoK: Layer-two blockchain protocols," in *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10-14, 2020 Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Bonneau and N. Heninger, Eds., vol. 12059. Springer, pp. 201–226. [Online]. Available: https://doi.org/10.1007/978-3-030-51280-4_12

[74] T. Neudecker and H. Hartenstein, "Short paper: An empirical analysis of blockchain forks in bitcoin," in *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*, ser. Lecture Notes in Computer Science, I. Goldberg and T. Moore, Eds., vol. 11598. Springer, pp. 84–92. [Online]. Available: https://doi.org/10.1007/978-3-030-32101-7_6

[75] K. Wüst, S. Matetic, M. Schneider, I. Miers, K. Kostiainen, and S. Capkun, "ZLiTE: Lightweight clients for shielded zcash transactions using trusted execution," in *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*, ser. Lecture Notes in Computer Science, I. Goldberg and T. Moore, Eds., vol. 11598. Springer, pp. 179–198. [Online]. Available: https://doi.org/10.1007/978-3-030-32101-7_12

[76] K. Wüst, K. Kostiainen, V. Capkun, and S. Capkun, "PRCash: Fast, private and regulated transactions for digital currencies," in *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*, ser. Lecture Notes in Computer Science, I. Goldberg and T. Moore, Eds., vol. 11598. Springer, pp. 158–178. [Online]. Available: https://doi.org/10.1007/978-3-030-32101-7_11

[77] T. Cao, J. Yu, J. Decouchant, X. Luo, and P. Veríssimo, "Exploring the monero peer-to-peer network," in *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10-14, 2020 Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Bonneau and N. Heninger,

Eds., vol. 12059. Springer, pp. 578–594. [Online]. Available: https://doi.org/10.1007/978-3-030-51280-4_31

[78] R. Pass and E. Shi, "The sleepy model of consensus," in *Advances in Cryptology – ASIACRYPT 2017*, ser. Lecture Notes in Computer Science, T. Takagi and T. Peyrin, Eds. Springer International Publishing, pp. 380–409.

[79] P. Wei, Q. Yuan, and Y. Zheng, "Security of the blockchain against long delay attack." [Online]. Available: https://eprint.iacr.org/2018/800

APPENDIX

The term *permissionless* is largely used to describe protocols that have the same or similar properties to Bitcoin. It hence follows that we should re-iterate over important goals and properties of the original Bitcoin whitepaper [14]. Hereby it is not our intention to analyze the fundamental properties of Bitcoin's protocol construction in detail, as there already exist numerous excellent works that formally discuss this topic [4], [5], [6]. We stress that this is our interpretation of the original intentions in light of a decade's worth of developments within this research field, as Bitcoin's authors remain pseudonymous and unavailable for further clarification to this date.

The core goal of the Bitcoin protocol is to allow parties to transact with each other while avoiding the double-spending problem without requiring a trusted third party, over the internet in a peer-to-peer setting. Participants should be able to join and leave the protocol execution at will and do not need to be identified, meanwhile their transactions should enjoy both temporal persistence and resistance to tampering. As stated by Nakamoto:

> "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

To this end, Bitcoin proposes a solution to the double-spending problem in a peer-to-peer network by establishing a distributed timestamping service to record an ordered public history of transactions that is based on proof-of-work, in which the majority of computational power is assumed to be controlled by honest participants.

a) Actor Roles: The actors, or nodes, within this system are allowed to join and leave the protocol execution at any time, and it is clearly distinguished between SPV nodes and full network nodes. The distinction between the two is made as SPV nodes do not perform a full verification of the correctness of the ledger state, and instead outsource some of this trust to full nodes under the assumption that the majority of computational power is controlled by honest nodes.

> "It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, ... He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it. As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker."

A further subtle differentiation between actor roles is made by considering the possibility that full nodes may discard previous spent transactions to reclaim disk space. This proposal raises interesting questions, as it opens up the possibility to a situation where all nodes may discard previous transactions, thereby preventing a new node from fully verifying the correctness of the ledger up to a particular point in time.

TABLE I. CATEGORIZATION RESULTS FROM STEP 5 OF THE HEREIN PROPOSED ANALYSIS METHOD (SEE SECTION II-A). THE SYMBOL ₿ REPRESENTS BITCOIN, Ξ REPRESENTS ETHEREUM, *PoS* STANDS FOR PROOF-OF-STAKE, *PoX* STANDS FOR PROOF-OF-X, *BFT* FOR BYZANTINE FAULT TOLERANCE, *Sci* SIGNIFIES EXAMPLES FROM ACADEMIA, *NC* STANDS FOR NAKAMOTO CONSENSUS, *CC* MEANS CRYPTOCURRENCIES, *ND* IS SHORT FOR 'NO DEFINED SET OF NODES', ✓SIGNALS THAT THE PAPER PROVIDES A DEFINITION, *no auth.* STANDS FOR 'NO AUTHORIZATION', *no IDs* FOR 'NO IDENTITIES' AND *no TTP* STANDS FOR 'NO TRUSTED THIRD PARTY'.

Paper	Year	Conference	Def.	Examples	Actors	write	read	execute	Trust	Privacy	Other
[15]	2019	SP			open						
[30]	2019	SP	✓		anonymous	anonymous, incentives, transactions			attacker, incentives, self interest	transactions, anonymous parties	
[31]	2019	SP	✓	₿, Ξ	ND, weak IDs						
[32]	2018	SP	✓	₿, PoX,Sci	sybils						
[33]	2016	SP		₿	join/leave						
[34]	2020	SP	✓	₿, Sci, BFT	join/leave, ND, sybils, no IDs, no auth., anyone	anyone, periodically, ordering, agree, transactions			no auth.	noregistration	consensus, p2p, network
[3]	2019	SP		₿	join/leave, ND, anyone	accountability, redact		anyone, fee, data	accountability, public, no TTP		broadcast, illicit, illegal, data, decentralized
[35]	2020	SP									
[36]	2020	CCS		NC							
[37]	2019	CCS		₿							
[38]	2019	CCS		₿							
[39]	2019	CCS		CC, PoX				no trust, entities, interact	transactions, interact,no TTP, verification		
[40]	2018	CCS	✓	₿, Ξ , CC	join/leave, ND				deviate, honest		
[41]	2018	CCS						no trust, entities, interact	interact, no trust		
[42]	2018	CCS		Ξ							
[43]	2018	CCS	✓	CC, BFT, Sci	join/leave, ND, open						
[44]	2017	CCS		₿, Ξ							
[45]	2017	CCS	✓	₿							
[46]	2017	CCS	✓	₿	join/leave			anyone, submit			
[47]	2016	CCS	✓	₿	no IDs, open				no auth.	no IDs	
[48]	2016	CCS	✓		join/leave, ND, sybils, open						
[49]	2016	CCS	✓		join/leave, ND, open			order, manipulate	transactions, order		
[50]	2019	CCS									
[51]	2018	CCS									
[52]	2019	CCS									
[53]	2019	USENIX		₿	open						
[54]	2019	USENIX			open						
[55]	2017	USENIX	✓	₿	join/leave, anyone	anyone, miners					consensus

TABLE II. (CONT.) CATEGORIZATION RESULTS FROM STEP 5 OF THE HEREIN PROPOSED ANALYSIS METHOD (SEE SECTION II-A). THE SYMBOL ₿ REPRESENTS BITCOIN, Ξ REPRESENTS ETHEREUM, *PoS* STANDS FOR PROOF-OF-STAKE, *PoX* STANDS FOR PROOF-OF-X, *BFT* FOR BYZANTINE FAULT TOLERANCE, *Sci* SIGNIFIES EXAMPLES FROM ACADEMIA, *NC* STANDS FOR NAKAMOTO CONSENSUS, *CC* MEANS CRYPTOCURRENCIES, *ND* IS SHORT FOR 'NO DEFINED SET OF NODES', ✓SIGNALS THAT THE PAPER PROVIDES A DEFINITION, *no auth.* STANDS FOR 'NO AUTHORIZATION', *no IDs* FOR 'NO IDENTITIES' AND *no TTP* STANDS FOR 'NO TRUSTED THIRD PARTY'.

Paper	Year	Conference	Def.	Examples	Actors	write	read	execute	Trust	Privacy	Other
[56]	2020	NDSS		₿, Ξ, PoS, Sci,BFT							
[57]	2019	NDSS	✓	₿, Ξ	ND, miners, rational	miners, update, state, fee, agree	miners, before mining, verification, transactions, block	fee, miners, execute	honest, incentives, rational, correct		p2p, network
[58]	2019	NDSS	✓	₿, Ξ, BFT	join/leave, anyone, pseudonymous	anyone, pseudonymous	anyone	smart contracts, anyone			public/private, permissioned/permissionless
[59]	2019	NDSS	✓	PoS	join/leave, different roles, users, public key, no authorization	honest, money, eventually, proportional to resource, append, verification, transactions	clients, transactions, verification		no TTP, transactions, no auth.		
[60]	2019	NDSS		Ξ, Sci							
[61]	2017	NDSS			different roles, miners, anyone	miners, malicious, reorder	anyone, verification, blocks, transactions		miners		
[62]	2018	NDSS	✓	₿, Ξ, PoS	join/leave			order, incentives	transactions, ordering, manipulation, miners, profit, verification, consensus		consensus
[63]	2020	NDSS									
[64]	2020	NDSS									
[65]	2019	NDSS									
[66]	2018	NDSS									
[6]	2017	CRYPTO	✓	₿	join/leave, ND, public key, accounts, adversary	miners, eventually, state, verification, transactions	miners, adversary, consensus	miners, anyone, adversary, verification, submit, exclude, liveness	miners, verification, transactions		consensus, network
[67]	2020	CRYPTO						order fairness			
[5]	2017	Eurocrypt	✓		join/leave, no IDs, sybils, no auth.				no auth., no TTP	no IDs	consensus
[68]	2019	Eurocrypt	✓	₿, Ξ	join/leave, ND						
[69]	2018	Eurocrypt	✓	CC, ₿, PoS, BFT	join/leave			liveness			consensus, decentralized
[70]	2020	Eurocrypt									
[71]	2020	FC		₿							
[72]	2020	FC		₿, PoS							
[73]	2020	FC			open						
[74]	2019	FC		₿							
[75]	2019	FC		₿							
[9]	2018	FC		₿, Ξ							
[76]	2019	FC									
[77]	2020	FC									
[78]	2017	Asiacrypt	✓	₿, NC, PoS	join/leave						consensus
[79]	2018	Asiacrypt									