

Poster: Accountable Processing of Reported Street Problems

Roman Matzutt
matzutt@comsys.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Jan Pennekamp
jan.pk@comsys.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Klaus Wehrle
wehrle@comsys.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

ABSTRACT

Municipalities increasingly depend on citizens to file digital reports about issues such as potholes or illegal trash dumps to improve their response time. However, the responsible authorities may be incentivized to ignore certain reports, e.g., when addressing them inflicts high costs. In this work, we explore the applicability of blockchain technology to hold authorities accountable regarding filed reports. Our initial assessment indicates that our approach can be extended to benefit citizens and authorities in the future.

CCS CONCEPTS

• **Security and privacy** → *Systems security*; • **Information systems** → *Information storage systems*.

KEYWORDS

street problems, accountability, consortium blockchain, privacy

ACM Reference Format:

Roman Matzutt, Jan Pennekamp, and Klaus Wehrle. 2023. Poster: Accountable Processing of Reported Street Problems. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, November 26–30, 2023, Copenhagen, Denmark. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3576915.3624367>

1 INTRODUCTION

The ongoing digitization of everyday life has benefited the emergence of crowdsensing applications, which allow monitoring a large area using customer devices [5]. Examples of crowdsensing include environmental monitoring [10], traffic anomaly detection [13], and contact tracing during the coronavirus pandemic [11].

Another application for crowdsensing is the distributed monitoring of *street problems*, such as potholes or other traffic obstructions, illegal trash dumps, graffiti, or other damages. Relying on citizens to report the issues they observe promises to (a) increase the covered area, (b) reduce the associated costs for city officials, and (c) enable a citizen-centered prioritization of identified issues.

However, current corresponding platforms illustrate that this application lacks a clear candidate for operating the required infrastructure in a binding and transparent manner. On the one hand, NGOs may operate corresponding platforms, potentially with a special focus such as bike lane safety [3] or tracking anonymous reports of sexual violence to identify and improve unsafe areas [15]. Unfortunately, constituting separate organizations implies that reports are not binding for the affected administrations that would

need to handle those reports. On the other hand, governments or municipalities may operate corresponding platforms themselves, e.g., using FixMyStreet Platform [12]. However, even if the official government bodies claim to commit to handling reports to those platforms, giving them complete control over the reports can undermine any perceived accountability via technical means. For instance, if an issue is deemed too expensive to fix, the municipality has a financial incentive to hide the issue from the broader public.

In this work, we propose an initial framework that resolves this tension and enables citizens to file their reports while ensuring that the responsible authorities can be held accountable for neglecting them. Our framework, the *accountable city report platform (ACRP)*, traces reports on a consortium blockchain that is jointly operated by independent municipalities and, optionally, additional NGOs. This way, reports are recorded immutably, i.e., municipalities can neither hide nor modify any report later on. The potential use of blockchain technology for active citizen participation has been explored before [1], but, to the best of our knowledge, these use cases do not currently consider data submitted by the citizens themselves.

2 OVERVIEW AND VALUE PROPOSAL

Figure 1 illustrates our target architecture: Citizens are enabled to file digital reports of street problems that require attention from the responsible municipality. This report contains all information required to address the issue. The municipality keeps track of reported issues locally, but tracks its state on a consortium blockchain. The blockchain is operated by a group of independent municipalities and, optionally, NGOs, but must be publicly readable and the operating nodes must accept citizen-submitted data. Finally, the report is released to the public to establish public accountability.

In the following, we discuss that this approach can increase both accountability and data quality but also raises new challenges.

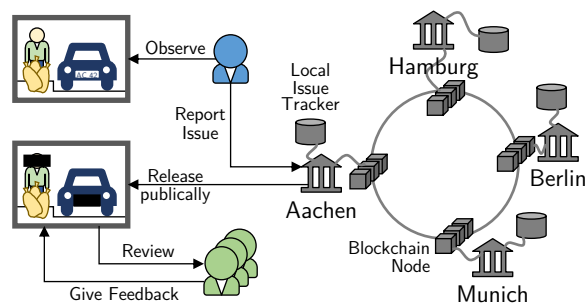


Figure 1: ACRP ensures that citizen-reported street problems are handled in an accountable manner.

CCS '23, November 26–30, 2023, Copenhagen, Denmark.

© 2023 Copyright held by the owner/author(s).

This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, November 26–30, 2023, Copenhagen, Denmark, <https://doi.org/10.1145/3576915.3624367>.

2.1 Benefits

The blockchain-backed and publicly observable approach of ACRP promises several advantages for both citizens and municipalities.

Accountability. The underlying blockchain can assert citizens that a trace of their filed reports is immutably recorded, i.e., the responsible authorities cannot deny having received any recorded report. This traceability extends to any subsequent handling of the report. As a result, reports cannot be altered or removed without due reason, which establishes the required accountability.

Reduced Duplicates. Blockchain-recorded data traces enable a globally agreed-upon view on the existence and current state of reports. Together with additional similarity checks, citizens and authorities can identify and merge potential duplicates more easily, reducing the workload for all involved entities.

Weighted Prioritization. Adding features such as up-voting or short comments in addition to the now-achievable transparency and deduplication further helps authorities assess and compare the *relevance* of identified street issues. Namely, citizens can better express the importance of individual issues, which allows authorities to optimize the achievable benefit for a given limited budget.

Citizen Mobility. Finally, a shared infrastructure facilitates mobile citizens, such as commuters or tourists. These groups would benefit from a unified interface to file reports about street problems relevant to their mobility patterns across different municipalities.

Overall, our approach promises benefits for citizens and municipalities. However, recording reports on a publicly readable blockchain comes with severe challenges, as we outline in the following.

2.2 Challenges

Despite the outlined benefits, our approach also creates new challenges ACRP must ultimately overcome for maximum acceptance.

Reporter and Citizen Privacy. Blockchain-recorded data has the potential to compromise the privacy of citizens, both directly [8] and indirectly [16]. Most notably, reports should include a photo to help authorities assess the legitimacy and extent of the issue. However, these photos may also include, e.g., bystanders' faces or license plates of nearby parked cars. For instance, Google's Street View raised various privacy concerns [14] and Google had to start blurring such information on a large scale [4]. Unfortunately, directly transferring this modification approach to blockchain-backed reports would interfere with the desired report accountability. Finally, reporters may indirectly disclose information about their individual points of interest via their reports' locations [17].

Data Quality. Reports are only valuable if they describe the issue at hand accurately enough so that the responsible authorities can take action. In addition to the privacy concerns discussed above, the *credibility* of submitted reports has to be ensured [7]. Since ACRP must provide an open platform for citizens, it must be able to handle reports that are (a) too low-quality to be actionable, (b) forged to provoke an unnecessary reaction with associated costs, and (c) "garbage" reports, e.g., containing spam or illicit content.

Usability. Crowdsensing approaches maximize their utility when more users are actively participating. As filing and handling reports inevitably introduces an overhead, achieving a good usability becomes crucial to not deter participation. Hence, filing a report must be simple and intuitive, even for citizens who are not tech-savvy. Furthermore, citizens must be presented an easy-to-navigate

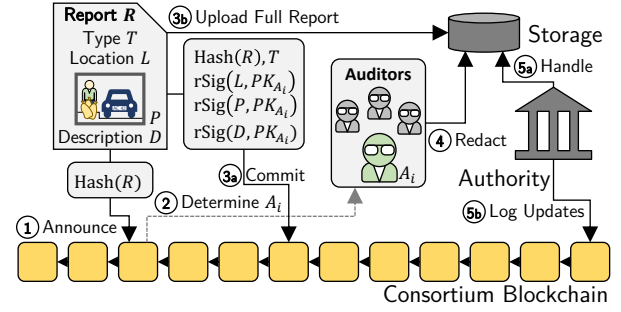


Figure 2: ACRP's blockchain keeps track of report states. Auditors can still moderate reports using redactable signatures.

list of relevant existing reports to facilitate the deduplication of similar reports (cf. Section 2.1). Finally, the different authorities must be able to receive, review, and respond in a timely manner when reports concerning their respective scope of duties are filed.

Next, we outline how ACRP currently addresses these challenges and where our early-stage approach requires further improvements.

3 ACCOUNTABLE REPORTING FRAMEWORK

We now outline ACRP's general approach for realizing moderation capabilities while retaining accountability and its report lifecycle.

3.1 General Approach

Citizens can file reports using their smartphone. In our initial design, each report is a tuple $R = (T, L, P, D)$, where T is the issue's *type*, L is a location, P is a picture of the issue, and D is a free-text description. The type is chosen from a fixed set of categories, such that (T, L) describes which authority is responsible for handling the report.

As street issues are a public concern, ACRP must establish accountability (cf. Section 2.1) but also provide moderation capabilities at the same time to be able to react to wrong or illicit information (cf. Section 2.2). To establish accountability, ACRP relies on a consortium blockchain where citizens and authorities log all actions related to announcing or handling issues. ACRP further realizes the required moderation by installing a set of semi-trusted *auditors* who vet and potentially redact incoming reports before they are published. Here, ACRP relies on *redactable signatures* [6], which allow dedicated parties to alter a signature's original message without invalidating the signature. This way, the auditors can redact reports without affecting the immutability of on-chain data.

3.2 Report Lifecycle

In the following, we provide further details about the lifecycle of any report, which consists of five steps as shown by Figure 2:

First, the citizen (1) announces the report by submitting $\text{Hash}(R)$ to the blockchain. The announcement does not disclose information about R but enables the citizen to prove its acceptance later on. ACRP can use this input and other blockchain information to pseudorandomly (2) determine a responsible auditor A_i [9]. Afterward, the citizen can select the public key for A_i and (3a) commit to R by submitting redactable signatures for L , P , and D to the blockchain. Simultaneously, the citizen (3b) uploads the full report to a dedicated storage. Next, the auditor can optionally redact R , yielding R' , without invalidating the on-chain signatures. If the auditor performs

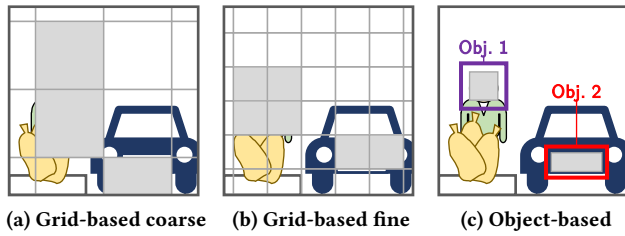


Figure 3: Chunking affects the performance and accuracy.

unwarranted redactions, the citizen can release the original report as evidence to resolve this dispute. Finally, the report is released to the public and the responsible authority, as determined by (T, L) , is asked to $\textcircled{5a}$ handle the report while $\textcircled{5b}$ logging all updates. Whenever reports must be completely discarded, either because they are not actionable by the authority or they cannot be published, the authority is still required to log a deletion action on the blockchain.

4 FIRST FEASIBILITY INSIGHTS OF ACRP

In this section, we assess the potential feasibility of ACRP by concluding that it achieves accountability and moderation at the same time and by discussing its overhead and usability implications.

Accountability vs. Moderation. A citizen initially only submits a hash value of their report R to the blockchain, i.e., its content is not leaked to the responsible authority, which could otherwise have an interest to reject R . Assuming that the blockchain network is not compromised by a large-scale attacker, its nodes will thus obviously accept the announcement of R . From this point onward, the citizen can always publish R to prove their submission of R and its initial content to third parties. Hence, the responsible authority has to react to the report. Using redactable signatures further only allows the auditor to remove, but not alter, parts of the report [6]. In the future, ACRP must further be hardened against other forms of unwanted user behavior, such as spamming reports.

Overhead. Keeping track of reports and potential redactions necessarily inflicts storage and processing overhead. However, we argue that this overhead is reasonable given the achievable benefits. Namely, storing only references to reports on-chain helps reducing the blockchain's growth rate and the redactable signatures per report comprise the bulk of the on-chain data. The redactable-signature scheme by Johnson et al. [6] assumes that the input message consists of multiple chunks and then yields signatures that grow logarithmically depending on message and chunk lengths and linearly depending on the number of redacted chunks. Furthermore, as illustrated by Figures 3a and 3b, the chunk size also determines the granularity available to the auditor, which could ultimately lead to necessary redactions that shadow a reported issue. Ideally, auditors were able to identify different objects of the report (Figure 3c) without large performance penalties. The assessment of available redaction schemes [2] as well as the chunking mechanisms are thus important future work to improve ACRP.

Usability. Having one decentralized backend for reporting street problems proves beneficial for mobile citizens as they can access ACRP from every supporting municipality. Establishing consensus about reported issues despite this decentralization further helps the desirable deduplication of reports because citizens can be

presented a more reliable list of potentially similar issues, i.e., of the same type in the same proximity. Extending this review process with social features such as up-voting or commenting registered reports then presents a valuable input for the prioritization on the authorities' end. However, ACRP's utility depends on how intuitive and easy filing and reviewing reports is and maximizing this utility in the future is crucial for increasing ACRP's acceptance.

In conclusion, ACRP's approach of combining blockchain-backed accountability with moderation capabilities due to redactable signatures is promising to facilitate the decentralized, accountable, and usable reporting of street issues by mobile citizens.

5 CONCLUSION

We proposed the accountable city report platform (ACRP) to increase the transparency of municipalities handling street problems such as potholes or illegal trash dumps. We identified a combination of blockchain-recorded meta information and redactable digital signatures as promising to establish this transparency, and thereby accountability, while retaining important moderation capabilities required for operating ACRP in the public. Our initial assessment suggests that we can extend ACRP to become a valuable tool for the modern city management. We are looking forward to exploring the requirements for realizing ACRP, and potential further use cases of its concept, in greater detail in the future.

REFERENCES

- [1] S. Ben Dhaou and J. Backhouse. 2020. Blockchain for smart sustainable cities. Tech. rep.
- [2] A. Bilzhaue et al. 2017. Position paper: the past, present, and future of sanitizable and redactable signatures. In *International Conference on Availability, Reliability and Security (ARES '17)*. ACM.
- [3] Cycling UK. 2007. Fill That Hole. last access: 2023-08-02. <https://www.fillthathole.org.uk>.
- [4] A. Frome et al. 2009. Large-scale privacy protection in Google Street View. In *International Conference on Computer Vision (ICCV '09)*. IEEE.
- [5] B. Guo et al. 2015. Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm. *ACM Comput. Surv.*, 48, 1, Article 7, (Aug. 2015).
- [6] R. Johnson et al. 2002. Homomorphic Signature Schemes. In *Topics in Cryptology (CT-RSA '02)*. Springer.
- [7] T. Luo et al. 2019. Improving IoT Data Quality in Mobile Crowd Sensing: A Cross Validation Approach. *IEEE Internet of Things Journal*, 6, 3.
- [8] R. Matzutt et al. 2018. A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In *Financial Cryptography and Data Security (FC '18)*. Springer.
- [9] R. Matzutt et al. 2020. Utilizing Public Blockchains for the Sybil-Resistant Bootstrapping of Distributed Anonymity Services. In *ASIA Conference on Computer and Communications Security (ASIACCS '20)*. ACM.
- [10] M. Mun et al. 2009. PEIR, the Personal Environmental Impact Report, as a Platform for Participatory Sensing Systems Research. In *International Conference on Mobile Systems, Applications, and Services (MobiSys '09)*. ACM.
- [11] S. Munzert et al. 2021. Tracking and promoting the usage of a COVID-19 contact tracing app. *Nature Human Behaviour*, 5, 2.
- [12] mySociety. 2012. FixMyStreet Platform. last access: 2023-08-02. <https://fixmystreet.org>.
- [13] B. Pan et al. 2013. Crowd Sensing of Traffic Anomalies Based on Human Mobility and Social Media. In *International Conference on Advances in Geographic Information Systems (SIGSPATIAL '13)*. ACM.
- [14] L. H. Rakower. 2011. Blurred Line: Zooming in on Google Street View and the Global Right to Privacy. *Brook. J. Int'l L.*, 37, 1, Article 8.
- [15] Red Dot Foundation Group. 2012. Safecity. last access: 2023-08-02. <https://www.safecity.in>.
- [16] F. Reid and M. Harrigan. 2013. An Analysis of Anonymity in the Bitcoin System. In *Security and Privacy in Social Networks*. Springer. Chap. 10.
- [17] J. H. Ziegeldorf et al. 2017. TraceMixer: Privacy-preserving crowd-sensing sans trusted third party. In *Annual Conference on Wireless On-demand Network Systems and Services (WONS '17)*. IEEE.