Towards Improving Accountability in Sensitive-Disclosure Scenarios

Roman Matzutt
roman.matzutt@fit.fraunhofer.de
Fraunhofer FIT
Sankt Augustin, Germany

Eric Wagner
eric.wagner@fkie.fraunhofer.de
Fraunhofer FKIE
Wachtberg, Germany

ABSTRACT

Public transparency has become increasingly important to uphold trust in government agencies and private companies alike, e.g., by establishing police accountability and proving abiding to ethical supply chain practices. Oftentimes, however, this public interest conflicts with the need for confidentiality of ongoing processes. In this paper, we investigate these *sensitive-disclosure scenarios* and the requirements for technical solutions to support the data dissemination in these scenarios. We identify *translucent* blockchains as a promising building block to provide transparency in sensitive-disclosure scenarios with fine-granular access control.

CCS CONCEPTS

• **Security and privacy** → *Human and societal aspects of security and privacy*; **Security services**.

KEYWORDS

Sensitive disclosure, accountability, transparency, blockchain

ACM Reference Format:
Roman Matzutt and Eric Wagner. 2024. Towards Improving Accountability in Sensitive-Disclosure Scenarios. In *European Interdisciplinary Cybersecurity Conference (EICC 2024), June 05–06, 2024, Xanthi, Greece.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3655693.3655715

1 INTRODUCTION

Blockchains have previously gained traction for general-purpose data-management applications due to their immutability, which helps establish transparency and accountability among mutually distrusting entities. Currently, blockchain systems are either *permissionless* or *permissioned*, promising full transparency to anybody or confining the access to the blockchain to selected participants, respectively. However, there is an increasingly important class of scenarios not covered by these designs at the moment: These are scenarios where transparency to the public is *eventually* desirable, but full transparency is counter-productive. For instance, exchanging information about ongoing developments regarding security vulnerabilities is crucial for effective responses and the public has a warranted interest to be informed in a timely manner about incidents affecting them [9]. However, full transparency to the public can backfire, as cybercriminals could be informed early as well and adopt their strategies accordingly. We refer to such scenarios as *sensitive-disclosure scenarios*, as transparent disclosure to the public is generally desirable, but extra precautions have to be taken to prevent negative consequences.

In this paper, we give an abstract characterization of sensitive-disclosure scenarios (Section 2). We then introduce the concept of *translucent blockchains* as a special type of permissioned blockchains with fine-granular policies for defining public accessibility of blockchain information (Section 3). Afterward, we show how translucent blockchains can be integrated into processes for handling sensitive-disclosure scenarios by discussing example use cases ranging from document unsealing to whistleblowing (Section 4). For our framework, we assume that the nodes maintaining a translucent blockchain can be trusted to follow these policies; however, we also discuss potential measures for restricting the possible misbehavior by single nodes (Section 5). Finally, we discuss related work (Section 6) before concluding this paper (Section 7).

Overall, translucent blockchains have the potential to become a suitable building block to address sensitive-disclosure scenarios.

2 SENSITIVE DISCLOSURE SCENARIOS

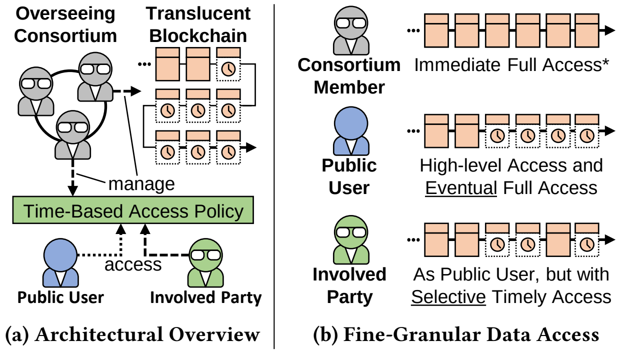
In this section, we first give our intuition behind sensitive-disclosure scenarios and then specify criteria suitable for identifying them within larger processes.

Sensitive-disclosure scenarios are fundamentally characterized by an inherent tension between warranted public interest and the need for (partial) confidentiality, as experts have to share data in a timely manner. Oftentimes, this tensed information asymmetry can be alleviated by introducing a time-based component: While the public should *eventually* be able to inspect all data, it can be tolerated when details are withheld for a time when the withholding can be legitimized by preventing negative consequences. Additionally, the information asymmetry can be modeled by adjusting the granularity of (immediately) published data, i.e., only relevant high-level data or aggregates can be released to the public immediately. Finally, the information asymmetry can be *subject to spontaneous change* based on unforeseen developments, such as large lawsuits of public interest, new regulation, or shifts in the public interest.

In summary, the following criteria should be given for sensitive-disclosure scenarios.

Public Interest. At the core of sensitive-disclosure scenarios lies a warranted interest by a large portion of the general public to access information that is otherwise considered confidential. Full access might not be relevant, but eventually the relevant documents have to be publishable to hold the relevant parties accountable.

EICC 2024, June 05–06, 2024, Xanthi, Greece
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1651-5/24/06
https://doi.org/10.1145/3655693.3655715



(a) Architectural Overview (b) Fine-Granular Data Access

Figure 1: Translucent blockchains implement fine-granular and time-constraint access policies.

Degrading and Partial Confidentiality. While the requested information is considered confidential, the public interest can be accommodated by a delayed or partial release. Partial releases can either consist of aggregates, such as relevant statistical data, or by releasing partially redacted documents.

Negotiable Disclosure. The exact means for public disclosure are defined and enforced by an authorized group of deciders. In addition to specific and publicly documented conditions for the disclosure of documents, these deciders must also be able to negotiate these conditions to react to new developments.

Based on this general framework, we now present the concept of translucent blockchains as a suitable technical building block for handling sensitive-disclosure scenarios and thereafter present how translucent blockchains can help realize a diverse set of use cases.

3 TRANSLUCENT LEDGERS

As discussed in Section 2, tackling sensitive-disclosure scenarios requires respecting the public interest of accessing partially confidential information with time-based and negotiable disclosure capabilities. We now argue that an adaption of well-known blockchain architectures can satisfy these partially conflicting requirements.

Blockchain architectures are traditionally either *permissionless* or *permissioned*. While anyone has write and read access to a permissionless blockchain, a permissioned blockchain is used by a known set of entitled parties with tunable policies for accessing blockchain information [25]. The free-access nature of permissionless blockchains renders satisfying the requirement for partial confidentiality (Section 2) challenging. Even though access policies can be realized by encrypting on-chain data [28], the need for fine-granular and time-based access control would introduce a considerable overhead regarding the key management [14]. Contrarily, permissioned blockchains are typically deployed in the form of *consortium blockchains*, which are only accessible by the agreed-upon *consortium members*; hence, these blockchains cannot satisfy the warranted public interest in the coordinated processes.

However, we observe that consortium blockchains can be slightly adjusted as shown in Figure 1a to form *translucent blockchains*, which can then satisfy the requirements imposed by sensitive-disclosure scenarios. Namely, consortium members should also accept data requests by non-members and respond according to a dedicated *outsider-access policy*. The outsider-access policy has two main components, (a) the age of the requested information and (b) the requesting user's role.

Via these two components, the consortium members can implement the fine-granular data access illustrated by Figure 1b. Consortium members have full access to on-chain data and trust each other to faithfully enforce the outsider-access policy, i.e., not leak information to unauthorized parties. In Section 5, we outline technical measures a consortium can take when individual members are not fully trustworthy. When an outsider requests information from a consortium member, that request is only served if permitted by the outsider-access policy, e.g., when enough time has passed such that the requested information is not considered sensitive anymore. If the requested information is still considered confidential, the user may at most obtain aggregate information, such as the number of ongoing confidential processes. A consortium can further operate a translucent blockchain as a service to handle sensitive-disclosure scenarios on behalf of third parties, such as responsible disclosure of cybersecurity vulnerabilities (cf. Section 4.2). In this case, the outsider-access policy must allow any party directly involved in the disclosure process full access to all relevant information.

After having outlined the concept of translucent blockchains with fine-grained access control, we next discuss related use cases.

4 USE CASES INVOLVING SENSITIVE DISCLOSURES

We now illustrate the prevalence of sensitive-disclosure scenarios as sub-problems in a diverse collection of use cases and outline how translucent blockchains can help in their respective contexts. These use cases involve *document unsealing* in general (Section 4.1), documenting processes that require short-term confidentiality but *eventual accountability* by the public (Section 4.2), and *whistleblowing* situations (Section 4.3).

4.1 Document Unsealing

Governmental transparency is a major factor of democracies [17]. Hence, governments have to define processes to implement this transparency. Due to the potential sensitivity of documents, governments typically define expiration dates for the "classified" status of those documents. For instance, the US by default declassify documents after 10 or 25 years depending on the documents' sensitivity, but also allow for more fine-grained control to shorten or prolong this period if deemed necessary [1]. Similarly, the EU follows a "thirty-year rule" as the default for declassification [8]; the premature declassification of documents may require consent from all involved entities and may require a joint decision in cases where the document's originating department no longer exists [2].

As such, translucent blockchains serve as a fitting building block to reliably digitize the process of document unsealing. Public users may file requests to declassify a document immediately. Any request can then be approved or denied via a joint vote of the consortium members. Furthermore, the consortium members agree upfront on a default period during which documents remain considered classified. This parameter is negotiable among the consortium members, and so is the labeling of different documents. Hence, translucent blockchain can also implement cases where documents have to remain classified for different durations. By releasing partial information, such as coarse meta information and statistics about ongoing voting activities, the consortium members can further increase the public's confidence in the decision-making about releasing or withholding information with a public interest.

Overall, translucent blockchains are a natural fit for document unsealing. In the remainder of this section, we discuss that they can also be applied in processes involving more complex roles.

4.2 Eventual Accountability

In Section 4.1, we outlined how governments could increase the public's trust by agreeing on timing policies regarding the declassification of documents. In that scenario, the consortium members are policymakers who oversee each other. Now, we discuss use cases where consortium members are in charge of recording processes involving third parties. As such, we discuss the applicability of translucent blockchains to support *police accountability* processes as well as *responsible disclosures* from the domain of cybersecurity.

Police Accountability. Maintaining a sufficient degree of transparency to the public as well as entertaining processes for establishing accountability are crucial for modern democratic policing agencies [13]. Policing agencies have to carefully gauge the acceptable level of transparency, as confidentiality breaches might interfere with ongoing investigations. Hence, ensuring police accountability constitutes another sensitive-disclosure scenario similar to document unsealing (cf. Section 4.1). In contrast to governments internally deciding whether to unseal documents, however, police agencies are increasingly controlled by *external* oversight bodies [13]. As such, the police agency must be assumed to act as one of multiple oversight bodies who would act as consortium members of a translucent blockchain for improving police accountability. In this scenario, individual police officers become external users who are involved with a subset of ongoing investigations; i.e., the officers require immediate access to related information whereas that information is legitimately withheld from public users (cf. Figure 1).

Responsible Disclosure. Leaving the field of governmental oversight, common best practices for disclosing cybersecurity vulnerabilities present another sensible-disclosure scenario: When security researchers identify vulnerabilities, they have an interest in quickly disseminating their findings to the public. Since such immediate disclosure also exposes the vulnerabilities to attackers, common vulnerability disclosure processes involve a confidentiality period, a mutually agreed-upon grace period for software developers to patch the vulnerability before it becomes known to a wider public [7]. Finding the right strategy for responsibly disclosing exploitable vulnerabilities remains a challenging case-by-case task.

Translucent blockchains can support such processes, as the consortium members can flexibly and selectively disclose information to the public. For instance, immediately published meta information may disclose the reporting entity and the affected software components. This way, security researchers create a public and retrospectively traceable trail of their disclosure process while confidentially exchanging information with the affected software developers. Furthermore, users of affected software components can be warned early in severe cases that require immediate mitigation steps, such as the 2021 Log4Shell vulnerability [9]. Finally, the consortium members can set a deadline for fixing the vulnerability upfront and disclose the full information after the deadline has passed or a fix has been rolled out. In its NIS 2.0 directive [10], the EU requires each of its member states to establish computer security incident response teams (CSIRTs), who shall cooperate and act as trusted intermediaries in a coordinated vulnerability disclosure. As such, the federation of CSIRTs provides a natural candidate for constituting the consortium of a translucent blockchain dedicated to the responsible disclosure of cybersecurity vulnerabilities.

In summary, translucent blockchains are promising for establishing eventual accountability where the reported data requires temporary confidentiality. Next, we consider sensitive-disclosure scenarios that also require reporter confidentiality.

4.3 Whistleblowing

Whistleblowing is a crucial tool for disclosing bad practices and other issues within an otherwise collaborative environment, e.g., an employee publishing covered-up information. Whistleblowing has the explicit goal of informing an outside organization or the general public and oftentimes seeks to enforce further investigations using the generated public pressure [18]. At the same time, the whistleblower intrinsically has to fear retribution as they violate non-disclosure rules and affect their colleagues or collaborators. Hence, whistleblowing platforms must be trusted to properly protect the whistleblower's privacy while facilitating follow-up investigations. In this section, we consider reporting *scientific misconduct* and *issues in supply chains* as two exemplary sensitive-disclosure scenarios related to whistleblowing and outline how translucent blockchains can help in those scenarios.

Scientific Misconduct. If researchers note forms of scientific misconduct, such as plagiarism or fabrication of research results, they should report the matter to promote good scientific practice. This reporting procedure constitutes a sensitive-disclosure scenario similar to responsible vulnerability disclosure (cf. Section 4.2). However, where responsible vulnerability disclosure has a collaborative nature to mitigate damage, reporting scientific misconduct is antagonistic in that one researcher accuses another. Furthermore, not all scientific misconduct is immediately provable and hence requires deliberation.

For instance, the German Research Foundation (DFG) defines its rules of procedure for dealing with scientific misconduct [12], which involves (a) confidential assessment of the report to substantiate its claims, (b) initially withholding the accuser's identity, (c) notifying the accused researcher of the initial findings and giving them the opportunity to defend themselves, and (d) a decision by vote among a committee of researchers. Furthermore, the procedure allows for consulting third parties in case their expertise is deemed necessary.

Translucent blockchains lend themselves to support this procedure where a federation of impartial research institutes may constitute the operating consortium and the accusing and accused researchers are considered involved parties with an asymmetric view on the temporarily confidential deliberation process. Hence, a translucent blockchain holds the potential for increasing the accountability of deliberation processes for deciding on scientific misconduct and further promote good scientific practice.

Supply Chain Management. Global supply chains continue to face serious issues such as forced labor or child labor; hence, regulators seek to increase the transparency of supply chains with debatable results [15]. In such scenarios, whistleblowers can play an important role in effectively unearthing unethical practices [20]. However, the whistleblower may fear retribution from their employer and thus require a platform to confidentially report their observations. A translucent blockchain can again support this sensitive-disclosure scenario by establishing a consortium of trusted oversight bodies and NGOs. Via the translucent blockchain, the consortium members can confidentially handle any reports and prepare an action, e.g., intensified auditing or a lawsuit, while selectively informing directly as well as indirectly affected companies within the supply chain without tipping off the investigated company. Due to the delayed release of the full information, the consortium can prove to the public that they enforce ethical supply chain practices.

In this section, we observed that translucent blockchains can support a wide range of sensitive-disclosure scenarios involving increasingly antagonistic external parties. However, enforcing the required fine-granular access policy relies on consortium members to be trustworthy and impartial. In the next section, we briefly discuss additional technical measures that can harden translucent blockchains against misconduct by individual consortium members.

5 POTENTIAL FOR IMPROVED SECURITY

In the base framework for translucent blockchains we outlined in Section 3, we assumed that consortium members and reporting entities (e.g., whistleblowers) are trustworthy. In this section, we outline potential violations of these assumptions as well as available building blocks for addressing these issues.

Information Leakage. The blockchain's underlying access policy toward external parties must be enforced by all consortium members. As all consortium members have full access to all blockchain data (cf. Figure 1b), a single member could violate the policy and leak confidential data to unauthorized external parties. Here, building blocks from the domain of threshold cryptography [11], e.g., based on Shamir's secret sharing [21], promise to limit the data accessible by individual consortium members. Using threshold cryptography, a reporter can submit information confidentially such that the consortium members have to jointly decrypt that data. While any data required during deliberation processes must be unsealed and is susceptible to leakage thereafter, threshold cryptography can help protect especially sensitive and only conditionally disclosed information. For instance, deliberation processes may require to know a whistleblower's identity to assess the credibility of their claim in exceptional cases, but their identity may remain secret in most of the cases.

Improper Responses. Consortium members may refuse to answer external users' requests to access information or return false responses. The distributed nature of a translucent blockchain already mitigates the impact of single uncooperative consortium members, as users can contact any member with their request. However, external users have no intrinsic means to verify the correctness of a response they receive. As one solution to this problem, the consortium members can publish all block headers without restriction and enable external users to validate the response using Merkle proofs [26], i.e., allow them to verify that the returned record is indeed recorded on the blockchain. Alternatively, the user can send their request to multiple consortium members simultaneously and identify false responses using majority voting [27].

Report Modification. Finally, a consortium member might attempt to alter a received report to interfere with the reporting user's intent or even harm them. The underlying translucent blockchain resolves any equivocation attempts by consortium members as part of the consensus algorithm. However, a consortium member can alter a report when initially contacted by the external user and prior to relaying it to other consortium members. Especially in scenarios that require reporter anonymity, a consortium member can try to impersonate the reporting user. To increase their confidence of correct report dissemination within the consortium, the user can make use of reliable broadcast primitives [6] to ensure that all consortium members, or a sufficiently large subset thereof, received the report as intended.

Hence, translucent blockchains hold further potential for future improvements that increase their utility in the face of individual untrustworthy consortium members.

6 RELATED WORK

Previous research efforts have considered the potential of blockchain technology transparently disclosing information related to increasingly complex processes.

Early on, notary services were established on top of Bitcoin to enable users to record cryptographic hash values on-chain to prove that they owned the document at the time the hash value was included on the blockchain [5]. While providing a potential basis for scenarios such as document unsealing or responsible vulnerability disclosure (cf. Section 4.2), notary services rely on the document owner to disclose their ownership. A translucent blockchain transfers control over the disclosure process to the consortium members, limiting the negative impact of uncooperative involved users.

Multiple works acknowledged that blockchains can help mediate the process of vulnerability disclosures. For instance, related work has proposed to establish blockchain-based bug bounty programs to ensure a fair compensation of reporting users [3, 16]. However, using a traditional blockchain model remains unsatisfactory when handling sensitive information about security vulnerabilities. Badash et al. [3] rely on a permissioned blockchain and encrypted on-chain exchanges, which promotes confidentiality but negates the potential public interest and does not fully seize the mediation potential offered by the blockchain-operating consortium members. Conversely, Hoffman et al. [16] proposed to operate a bug bounty program on top of Ethereum as a permissionless blockchain and IPFS. As details are only released to IPFS after fixing the reported bug, this approach is not applicable in nuanced cases of responsible vulnerability disclosure, such as the selective release of information about Log4Shell (cf. Section 4.2). More closely related to our envisioned approach, Lisi et al. [19] propose to effectively model translucent blockchains by establishing a private blockchain among trusted authorities and writing data to a public blockchain using an inter-blockchain bridge.

Supporting whistleblowers was another area of interest of blockchain researchers [22, 24]. However, these approaches focus on protecting the dissemination of whistleblowing files and the accuser's anonymity. Here, using a translucent blockchain allows for more control when handling accusations in scenarios where a trustworthy consortium that acts as an intermediary and will not censor the whistleblower can be identified.

Finally, blockchain systems were proposed to provide accountability in the context of supply chains [4, 23], but these approaches focus on accountable tracking and tracing procedures instead of confidentially reporting ethical concerns.

Hence, we are confident that the concept of translucent blockchains provides a valuable addition to the toolkit for addressing sensitive-disclosure scenarios.

7 CONCLUSION

In this paper, we identified sensitive-disclosure scenarios as conflict-ridden situations where data disclosure is of a wider public interest, but uncontrolled disclosure may inflict serious harm. Different sensitive-disclosure scenarios range from governmental unsealing of previously confidential over the responsible disclosure of security vulnerabilities to whistleblowing activities. We proposed translucent blockchains as a technical building block for supporting sensitive-disclosure scenarios by allowing the consortium members of an otherwise permissioned blockchain to selectively disclose information to external users based on an agreed-upon access policy. We are eager to explore additional use cases and challenges of this building block in future work.

ACKNOWLEDGMENTS

This research has been supported by the German Federal Ministry of Education and Research (BMBF) under grant number 01IS21100A. The responsibility for the content of this publication lies with the authors.

REFERENCES

[1] 2009. Exec. Order No. 13,526—Classified National Security Information. *Federal Register* 75, 2 (2009), pp. 707–731. https://www.archives.gov/files/isoo/pdf/cnsi-eo.pdf

[2] Administrative Committee of the European Court of Auditors. 2023. Delegated Decision No 17-2023 of the Administrative Committee of the European Court of Auditors of 1 March 2023 on implementing rules for handling RESTREINT UE/EU RESTRICTED information at the European Court of Auditors. *Official Journal of the European Union* L, 86 (2023), pp. 65–82. http://data.europa.eu/eli/proc_rules/2023/17/oj

[3] Lital Badash, Nachiket Tapas, Asaf Nadler, Francesco Longo, and Asaf Shabtai. 2021. Blockchain-Based Bug Bounty Framework. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing (SAC'21)*. ACM, pp. 239–248. https://doi.org/10.1145/3412841.3441906

[4] Lennart Bader, Jan Pennekamp, Roman Matzutt, David Hedderich, Markus Kowalski, Volker Lücken, and Klaus Wehrle. 2021. Blockchain-Based Privacy Preservation for Supply Chains Supporting Lightweight Multi-Hop Information Accountability. *Information Processing & Management* 58, 3 (2 2021). https://doi.org/10.1016/j.ipm.2021.102529

[5] Massimo Bartoletti and Livio Pompianu. 2017. An Analysis of Bitcoin OP_RETURN Metadata. In *Financial Cryptography and Data Security (FC)*, Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson (Eds.). Springer Cham, pp. 218–230.

[6] Gabriel Bracha. 1984. An Asynchronous $\lfloor (n-1)/3 \rfloor$-Resilient Consensus Protocol. In *Symposium on Principles of Distributed Computing (PODC)*. ACM, pp. 154–162. https://doi.org/10.1145/800222.806743

[7] Hasan Cavusoglu, Huseyin Cavusoglu, and Srinivasan Raghunathan. 2007. Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge. *IEEE Transactions on Software Engineering* 33, 3 (2007), pp. 171–185. https://doi.org/10.1109/TSE.2007.26

[8] Council of the European Union. 2003. Council Regulation (EC, Euratom) No 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community. *Official Journal of the European Union* L, 243 (2003), pp. 0001–0004. http://data.europa.eu/eli/reg/2003/1700/oj

[9] European Network and Information Security Agency (ENISA). 2021. *Joint Statement on Log4Shell*. https://www.enisa.europa.eu/news/enisa-news/statement-on-log4shell Accessed on 2024-01-26.

[10] European Parliament and Council of the European Union. 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *Official Journal of the European Union* L, 333 (2022), pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555

[11] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. 2007. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *Journal of Cryptology* 20, 1 (2007), pp. 51–83. https://doi.org/10.1007/s00145-006-0347-3

[12] German Research Foundation. 2019. *Rules of Procedure for Dealing with Scientific Misconduct*. Technical Report. https://www.dfg.de/de/verfahrensordnung-zum-umgang-mit-wissenschaftlichem-fehlverhalten-verfowf--246936

[13] Emmanuel-Pierre Guittet, Niovi Vavoula, Anastassia Tsoukala, and Monika Baylis. 2022. *Democratic Oversight of the Police*. Technical Report. https://www.europarl.europa.eu/committees/en/democratic-oversight-of-the-police/product-details/20220606CAN66202

[14] Martin Henze, René Hummen, Roman Matzutt, Daniel Catrein, and Klaus Wehrle. 2013. Maintaining User Control While Storing and Processing Sensor Data in the Cloud. *International Journal of Grid and High Performance Computing (IJGHPC)* 5, 4 (12 2013), pp. 97–112. https://doi.org/10.4018/ijghpc.2013100107

[15] David Hess. 2019. The Transparency Trap: Non-Financial Disclosure and the Responsibility of Business to Respect Human Rights. *American Business Law Journal* 56, 1 (2019), pp. 5–53. https://doi.org/10.1111/ablj.12134

[16] Alex Hoffman, Eric Becerril-Blas, Kevin Moreno, and Yoohwan Kim. 2020. Decentralized Security Bounty Management on Blockchain and IPFS. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC'21)*. IEEE, pp. 241–247. https://doi.org/10.1109/CCWC47524.2020.9031109

[17] James R. Hollyer, B. Peter Rosendorff, and James Raymond Vreeland. 2011. Democracy and Transparency. *The Journal of Politics* 73, 4 (2011), pp. 1191–1205. https://doi.org/10.1017/S0022381611000880

[18] Peter B. Jubb. 1999. Whistleblowing: A Restrictive Definition and Interpretation. *Journal of Business Ethics* 21 (1999), pp. 77–94. https://doi.org/10.1023/A:1005922701763

[19] Andrea Lisi, Prateeti Mukherjee, Laura De Santis, Lei Wu, Dmitrij Lagutin, and Yki Kortesniemi. 2022. Automated Responsible Disclosure of Security Vulnerabilities. *IEEE Access* 10 (2022), pp. 10472–10489. https://doi.org/10.1109/ACCESS.2021.3126401

[20] Gerald G. Moy. 2018. The role of whistleblowers in protecting the safety and integrity of the food supply. *npj Science of Food* 2, 8 (2018). https://doi.org/10.1038/s41538-018-0017-5

[21] Adi Shamir. 1979. How to Share a Secret. *Commun. ACM* 22, 11 (1979), pp. 612–613. https://doi.org/10.1145/359168.359176

[22] Antonio Emerson B. Tomaz, José Cláudio do Nascimento, and José Neuman de Souza. 2022. Blockchain-based whistleblowing service to solve the problem of journalistic conflict of interest. *Annals of Telecommunications* 77 (2022), pp. 101–118. https://doi.org/10.1007/s12243-021-00860-0

[23] Eric Wagner, Roman Matzutt, Jan Pennekamp, Lennart Bader, Iraki Bajelidze, Klaus Wehrle, and Martin Henze. 2022. Scalable and Privacy-Focused Company-Centric Supply Chain Management. In *Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2022)*. IEEE. https://doi.org/10.1109/ICBC54727.2022.9805503

[24] Huaqun Wang, Debiao He, Zhe Liu, and Rui Guo. 2020. Blockchain-Based Anonymous Reporting Scheme With Anonymous Rewarding. *IEEE Transactions on Engineering Management* 67, 4 (2020), pp. 1514–1524. https://doi.org/10.1109/TEM.2019.2909529

[25] Karl Wüst and Arthur Gervais. 2018. Do you Need a Blockchain?. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, pp. 45–54. https://doi.org/10.1109/CVCBT.2018.00011

[26] Mingchao Yu, Saeid Sahraei, Songze Li, Salman Avestimehr, Sreeram Kannan, and Pramod Viswanath. 2020. Coded Merkle Tree: Solving Data Availability Attacks in Blockchains. In *Financial Cryptography and Data Security*, Joseph Bonneau and Nadia Heninger (Eds.). Springer International Publishing, Cham, pp. 114–134.

[27] Jan Henrik Ziegeldorf, Roman Matzutt, Martin Henze, Fred Grossmann, and Klaus Wehrle. 2018. Secure and anonymous decentralized Bitcoin mixing. *Future Generation Computer Systems* 80 (2018), pp. 448–466. https://doi.org/10.1016/j.future.2016.05.018

[28] Guy Zyskind, Oz Nathan, and Alex 'Sandy' Pentland. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *2015 IEEE Security and Privacy Workshops*. pp. 180–184. https://doi.org/10.1109/SPW.2015.27