Implementing blockchain logging for the Inverse Transparency toolchain with P³
Bachelor's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Valentin Zieglmeier
Email: {pretschn, ziegelm}v@in.tum.de
Phone: +49 (89) 289 - 17834

Starting date: immediately

Context
To give employees more sovereignty over how their data are used, the concept of Inverse
Transparency was introduced. Its core idea is to monitor all accesses to data and make those
logs visible (transparent) to data owners [1]. On the one hand, this can help raise awareness
of data usages and better protect employee's personal data, on the other hand it may enable
usages of data useful to teams and individuals alike.

A prerequisite for Inverse Transparency to function is the ability to record usage logs in a
tamper-proof way. Ideally, this can be done without a trusted third party, as in power-asymmetric
environments the logs may be the target of manipulation. Blockchain promises to enable this.
Previously, blockchain-based distributed secure logs were introduced (e.g., [2, 3]). There are
advantages of these applications, with a lightweight way to guarantee immutability of stored
entries (integrity) that functions even in unreliable distributed networks (availability). Yet, existing
solutions are either not GDPR-compliant or are not applicable in our case. Accordingly, we
have introduced a concept for blockchain-based logging for secure usage logs with P³ [4]. In
contrast to related work, it does not require a trusted third party or adaptations of the underlying
blockchain software.

Goal
The goal of this work is to implement the proposed concept and evaluate its feasibility in practice.
That encompasses three parts: Theoretical research, implementation, and evaluation.

Theoretical research. The P³ concept addresses integrity and non-repudiation in light of
GDPR requirements. Importantly though, practical considerations such as logging speed,
hardware requirements, etc. are not discussed. This thesis will deliberate each aspect of the
logging concept in theory, including but not limited to peer-to-peer communication and which
blockchain software to choose, and outline the implications of these implementation choices.

Implementation. The core contribution of the thesis is to implement the P³ system. In the
conceptual architecture, the system could supplant the Overseer component (see [1]). That
means that it should provide the same incoming and outgoing API as Overseer. The exact
relationship to other components and embedding in the toolchain will be discussed and adapted
to the findings of the theoretical research. Apart from that, requirements are given by the
existing concept (see [4]).

Evaluation. The evaluation will comprise a theoretical analysis of the security and practicality
of the implementation compared to the theoretical concept, as well as performance and system
load measurements under various expected loads.

Work Plan
1. Research related literature.
2. Implement the P³ system.
3. Analyze security implications of implementation choices and evaluate performance.

Deliverables
• Source code of the implementation.
• Thesis written in conformance with TUM guidelines.

References
Implementing blockchain logging for the Inverse Transparency toolchain with P

