# Masters‘ Thesis

# Scalability of Privacy-Preserving Off-Chaining Approaches

Blockchain technology finds increasing adoption in different application domains, e.g., energy, in real-world projects, e.g., BloGPV [1]. Several projects identified a high need for preserving privacy while using permissionless blockchain technology.

One of the most promising ways to address these privacy needs is off-chaining using Zero-Knowledge Proofs. Generating Zero-Knowledge Proofs, however, is a demanding computation that does not scale well with increasing complexity, which can significantly impair the adoption of this approach.

This thesis addresses the problem of scalability of proof generation using the ZoKrates toolbox (for the Ethereum blockchain technology). A first approach for doing so that comes to mind is generic distributed proof generations [2]. However, it is nontrivial to do so. Thus, this thesis approaches the problem from another angle: "smart" design and distributed execution of ZoKrates programs. What does this mean? ZoKrates programs commonly translate to several invariants
that require a local or global state. We envision generating different ZoKrates programs that group local and global invariants that evaluate to sub-proofs and allow for "easy" parallel computation.

In the context of this thesis, corresponding development tools for splitting and merging sub-proofs are to be developed and evaluated by comparison with an existing centralized prototype from the project BloGPV.

**Contact: Jörn Kuhlenkamp**
**jk@ise.tu-berlin.de**

[1] https://blogpv.net/
[2] https://www.usenix.org/conference/usenixsecurity18/presentation/wu

**Our Mission:**
Our lectures cover fundamental methods and techniques in the areas of service computing, cloud computing, and enterprise computing. We like to engage students in hands-on building of distributed information systems and to take an interdisciplinary approach to evaluating such systems. Through a close mentoring of students, especially in our seminars, we aim to introduce students to our ongoing research and to excite them to do future studies and research with us.

ISEngineering
Wirtschaftsinformatik –
Information Systems Engineering