Abuse-resistant pseudonymization and pseudonym change without trusted third parties

Martin Florian, Ingmar Baumgart
Institute of Telematics
Karlsruhe Institute of Technology (KIT)
76131 Karlsruhe, Germany
Email: {florian,baumgart}@kit.edu

I. Introduction

Privacy-preservation is becoming increasingly important as more and more areas of life are benefiting from the ubiquitous interconnection of humans and autonomous devices. At the same time, allowing users (and their devices) to collaborate and use services anonymously can lead to abuse, degrading the utility of novel systems and services. Additionally, without limiting access in some form, *sybil attacks* become possible where adversaries create large numbers of fake virtual identities (*sybils*). This both enhances the potential magnitude of abuse and enables malicious users to avoid blacklisting.

The issuing of unlinkable *pseudonyms* to users is a common solution to the challenge of hiding user identities while enabling access control and the effective protection against sybil attacks. Additionally, unlinkable *pseudonym changes* must be made possible for reducing the linkability between (potentially privacy-relevant) data samples originating from the same user.

Established approaches for enabling sybil-resistant *pseudonymization and pseudonym change* (PPC) inherently require a *trusted third party* (TTP) like a certification authority for enforcing issuing criteria and preventing sybil attacks. Upon compromise of the TTP, large-scale sybil attacks become possible and the trustworthiness of issued pseudonyms is greatly reduced. Thus, centralized pseudonym issuers become attractive targets for attacks, resulting in high operational costs for maintaining their security. Additionally, the notion of universal trust anchors shared by all system participants is questionable when considering mobile users in a globally interconnected world.

II. Contributions

As an alternative to assuming centralized TTPs, we explore the use of distributed, non-malleable bulletin boards as provided by cryptocurrency block chains. Our contributions so far are the following:

- A novel approach towards TTP-free and abuse-resistant pseudonymization and pseudonym change (PPC). To the best of our knowledge, we are the first to propose a complete PPC system that both prevents sybil attacks and doesn't rely on a TTP for ensuring the correctness and security of any of its operations.
- A specific implementation of the approach - *BitNym* - leveraging the existing *Bitcoin* network without requiring any modifications to its underlying protocols.
- A prototype of the proposed system and an evaluation of our approach using simulations of user populations and pseudonym changing behavior.

III. General Approach

Our PPC approach is based on three central building blocks: *genesis pseudonym creation*, *pseudonym change* and *pseudonym validation and use*. A central challenge we tackle is to ensure the resistance to sybil attacks in all three building blocks while remaining independent of TTPs.

At the core of our approach, *pseudonyms* are encoded in the outputs of cryptocurrency transactions. The *validity* of a pseudonym is determined based on the existence of a correctly formed transaction chain to a valid *genesis pseudonym transaction* (GPTx). Such a *validation path* is depicted in Fig. 1. Every GPTx encodes a proof that a predefined set of issuing criteria have been met by a user. For ensuring the unlinkability of pseudonyms and allowing unlinkable pseudonym changes, we adapt state of the art techniques for anonymizing cryptocurrency transactions for realizing *pseudonym mixing*.

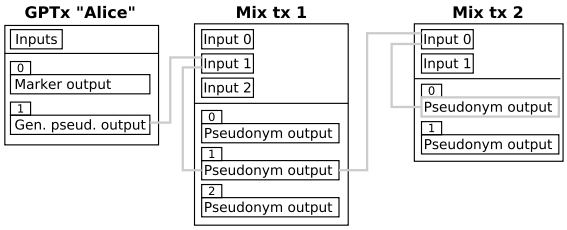

Fig. 1. GPTx created by Alice and validation path involving that transaction. The validated pseudonym is not necessarily held by Alice.

IV. Future work

We view the presented work as a base for a wide range of further works. Amongst other things, we plan to further investigate social-graph based initial access control for BitNym. Additionally, we will design and evaluate specific blacklisting mechanisms and investigate to what extend reputation scores can be introduced without breaking anonymity.