

Tutela: An Anonymity Tool for Ethereum and Tornado Cash

Mike Wu[†], Will McTighe[‡], Kaili Wang[†]

Department of Computer Science[†]

Graduate School of Business[‡]

Stanford University

{wumike, wmctighe, kkwang22}@stanford.edu

Abstract

A common misconception among blockchain users is that decentralization guarantees privacy. The reality is almost the opposite as every transaction one makes, being recorded on a public ledger, reveals information about one's identity.

1 Introduction

TODO

2 Tutela Overview

TODO

3 Data and Setup

TODO

4 Ethereum Heuristics

4.1 Deposit Address Reuse

4.2 Diff2Vec

5 Tornado Cash Heuristics

5.1 Address Match

5.2 Unique Gas Price

5.3 Multiple Denomination

5.4 Interaction History

6 History and Roadmap

7 Discussion

7.1 Limitations

7.2 Extensions

7.3 Broader Impact