Contents

1 Introduction **3**

2 Ease of Use through Lightweight Identity **3**
- 2.1 Address-Based Encryption . . . 4
  - 2.1.1 Single-Node Address-Based Encryption . . . 4
  - 2.1.2 Drawbacks . . . 4
  - 2.1.3 Distributed Scheme . . . 5
  - 2.1.4 Summary of Operations . . . 5
- 2.2 Aggregating Reputation Signals through Encrypted EigenTrust . . . 6
  - 2.2.1 EigenTrust . . . 6
  - 2.2.2 Privacy-Preserving EigenTrust through Zero-Knowledge Proofs . . . 7
  - 2.2.3 Personalized Pre-Trusted Peers . . . 7
  - 2.2.4 Practical Implications . . . 7

3 Stabilizing Value **7**
- 3.1 Elastic Coin Supply and Shifting Volatility Risk . . . 8
- 3.2 Protocol Summary . . . 8
- 3.3 Shared Reserves . . . 9
- 3.4 Price Discovery and Mechanics of Reserve Asset Purchasing . . . 10

4 Governance and Incentives **10**
- 4.1 Maintaining the System . . . 10
- 4.2 Bolstering Reserves and Contracting Stable-Value Currency Supply when Needed . . . 11
- 4.3 Increasing User Base and Usage of the System . . . 11
- 4.4 Improving the Protocol . . . 11
  - 4.4.1 Technical Improvements . . . 11
  - 4.4.2 Introducing Regional Currencies and Broadening the Reserve Base . . . 12
  - 4.4.3 Futarchical Governance . . . 12
  - 4.4.4 Partitioned Reserves . . . 12

5 Conclusion **13**