each iteration, each node send across their $t_i \cdot T_{ij}$ scores to each node j that they've paid in the past. The nodes j wait to receive all of the scores from the nodes that have paid them in the past, and then compute their own t_j, and then pass their $t_j \cdot T_{jk}$ along to the nodes k that they have paid.

2.2.2 Privacy-Preserving EigenTrust through Zero-Knowledge Proofs

There are two differences between the algorithm we propose and the original EigenTrust algorithm.

First, the simplified description above allows nodes to lie about their own t_i. The original EigenTrust algorithm addresses this by relying on score managers to steward the computation of t_i for each node. In the original scheme, each node has three score managers, assigned at random through a distributed hash table, who store the T_{ij} values for each node and compute and store t_i for each node. While this addresses the dishonest node attack, it is not ideal in the social payments scenario, as it requires sharing transaction information with other peers in the network. We address this by having each peer perform the computation themselves, as per the simplified version, but also prove, to a high probability, to all adjacent nodes that they have performed the computation correctly. One can do so by constructing a zero-knowledge proof using a variety of cryptographic means, including [10, 3, 5].

2.2.3 Personalized Pre-Trusted Peers

Second, in order to break malicious cliques, and to ensure convergence of the power method and uniqueness of the principal eigenvector, EigenTrust introduces the notion of pre-trusted peers, a group of peers that are active and assumed to be universally trusted. This ensures that the graph is acyclic and strongly connected (and that the matrix is irreducible and that the problem is well-conditioned). However, it requires the system to define a set of universally trusted peers, and concentrates outsized power to confer reputation in those pre-trusted peers.

We can address this through personalization. Rather than computing a single global reputation vector, the system can compute a personalized global reputation vector for each peer, that gives the reputation score of each peer j in the network from the point of view of a single peer i. To compute personalized EigenTrust for peer i, one can simply perform a traditional EigenTrust computation, but use the contact list of peer i as the set of pre-trusted peers.

This is far more computationally expensive than a single EigenTrust computation; however, we apply many of the computation-saving techniques that enabled personalized PageRank [13] to a personalized EigenTrust computation.

2.2.4 Practical Implications

For the social payments case, in which people text money to friends, the address-based encryption scheme suffices as a lightweight identity proxy, allowing people to send money directly to people's cell phone numbers, even if they have not signed up for a wallet.

As people are interested in using the protocol to pay people outside of their direct circle of contacts, it is useful for a user to be able to aggregate the trust signals of those in their network to make purchase, payment, and credit decisions, and to mitigate bad actors.

Further, a reputation scheme as we described enables a more robust identity scheme. Most identity schemes are based on attestations from others, and it would be useful to be able to weight those attestations by the reputation score of the attestor.

3 Stabilizing Value

Perhaps the biggest hurdle to the use of cryptocurrencies as a means of payment is their volatility. Consumers are unlikely to want to buy a volatile cryptocurrency to spend it, since the purchasing power of their accounts would fluctuate widely with market demand for the currency. Merchants who accept cryptocurrencies are likely to convert to fiat upon payment, because their business model does not involve speculating on cryptocurrencies. And the most successful cryptocurrencies today are not just volatile but deflationary – their success leads to their price rising; as a result, prices denominated