Read.me

Proof of Solvency provides a verifiable audit of possession over a given amount of funds at a given time to cryptocurrency custody providers and third parties, including their customers, to show proof of properly storing customer funds.
The service is open source and sets standards of greater transparency, accountability and trust in the digital currency industry.

The URL to working application:
http://ec2-3-120-37-108.eu-central-1.compute.amazonaws.com:3000/
- The URL to your public github repository:
https://github.com/tensiv/PROTOTYPE

Description
Proof of Solvency is a service designed to let users verify the solvency of websites, which accept cryptocurrency deposits (e.g. exchange websites, online wallets, gambling websites, etc.) in a way that does not compromise the privacy of users.
The auditing process consists of three individual steps: summing the user account balances (proof of liabilities), summing the assets, i.e., address balances, the exchange controls (proof of reserves), and proof that the reserves cover the liabilities (proof of solvency).

Proof of liabilities
For the proof of liabilities, the custody service provider (e.g. exchange) prepares a list with the account holder IDs and the according balances and uploads it through a form provided by us. After having parsed the list, we calculate hashes of the customer IDs and the balances. Based on that we build a merkle tree, as it is an efficient way to store the data and secure the privacy of each account holder. We recommend publishing the root of the merkle tree to make accessible for everyone.

Proof of reserves
For the proof of reserves the custody services provider (e.g. exchange) inserts a lists with all addresses the own, their balances and the according signatures. To proof that the exchange owns one address it signs a unique message given by us with the according private key. The private key is only known to the exchange. We verify the signed message connect to a block explorer and add up all the balances of verified addresses. This gives us the sum of all the assets owned by the custody service provider.

Proof of solvency
To prove the solvency we subtract the sum of liabilities from the sum of assets. A positive result is indication for solvency. As this is a tool for the account holder to audit the exchange we give her a way to prove the solvency and check if her account was included in the audit.

Therefore, we built a website where an account holder can type in her data consisting of the account holder ID and the balance at the time of the audit. After filling it in the credentials the user sees if her account was included. We give each user her hash and the merkle tree path. With both values the merkle root can be calculated (it can be done be herself as well). The account was included in the solvency proof if the new merkle root is the same as the published one based on the proof of reserves. The result is displayed over our web service
The more customers prove it, the more confident they can be that the exchange is solvent.

Next steps

- Include zero-knowledge proofs. So exchanges do not need to disclose the number of account holders and their balances
- Include different cryptocurrencies
- Build connections to different wallet providers for easier processes