“Our platform is a paperless and trustless way to secure your precious seed phrases.”

The idea is an implementation of *Shamir’s Secret Sharing Algorithm.* The algorithm with split your seed phrase into multiple pieces that can be stored separately.

The platform has 2 parts:

The first part is how to backup the seed phrase

To backup a seed phrase, a user logs in to our web-app, enters a username and password to register and submits us the seed phrase. The seed phrase is encrypted using the password and converted into pieces using *Shamir’s Algorithm.* Then a subset of nodes is selected from the set of registered nodes on the network.

Each selected node is sent a piece of the generated pieces. These pieces are first encrypted using the public keys of the selected nodes and then sent to them. Each node then decrypts them using their private key and stores the piece as a key-value pair; the value being the piece and the key being a string generated by encrypting the concatenated string of the user’s and the node’s usernames.

The pieces generated by S*hamir’s algorithm* are stored on mobile devices who register to become nodes on our network. To become a node, you download our app of the play store/app store. The app requires you to login with a username and password but doesn’t require any further interactions. It will run in the background and each user registered as a node receives some amount of money in exchange for lending us their mobile devices RAM and storage services.

When a user registers as a new node, a private key-public key pair is generated for encrypted messaging on the network. The private key is stored on the user’s device, the public key is stored on the server/ smart-contract.

The second part is how to retrieve the seed phrase

When a user logs in to retrieve their seed phrase, a request is sent to all the nodes to send their pieces to that user. Once the user receives these pieces, he decrypts them with his password. Then they combine the decrypted pieces using *Shamir’s Algorithm* to retrieve their seed phrase.

With each request for a seed phrase, the user generates a temporary private-key and public-key pair. The public key is sent to each node to encrypt their piece with. When the user receives the piece, it is first decrypted using the private key before being decrypted using the password.

FAQ

Q) Why the encrypted messaging?

When the pieces are circulating over the server, they are vulnerable to being attacked by hackers. So we used *RSA public private key strings* to encrypt all messaging over the network.

Q) Why will people download the app?

It pays the people in exchange for lending us a part of their storage

Q) How will you pay the people who download your app?

The revenue comes from the people who want to use our services to backup their seed phrases. Our mode of payment is Dai. Since it is a stable coin, people skeptic of using crypto currencies will not shy from signing up.