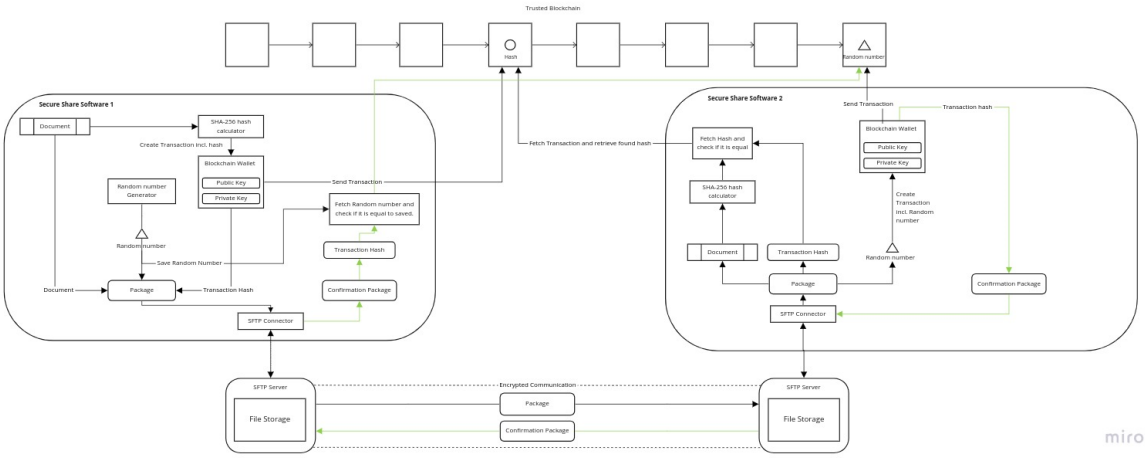
Architecture Flow:
Entity 1 wants to send a Document to Entity 2.

1. The software 1 of Entity 1 hashes the Document.
2. Software 1 creates a transaction containing the hash of the Document and sends a transaction (signed with its private) to the blockchain.
3. Software 1 generates a random secret.
4. Software 1 sends the document, random secret and the Transaction Hash (from the transaction that contained the hash) in a secure channel over SFTP to the SFTP server of Entity 2.
5. When the SFTP server of Entity 2 gets an entry, Software 2 will hash the received Document.
6. Software 2 will look up the received transaction hash in the blockchain and will extract the contained hash.
7. The hash that Software 2 generated from the Document will be compared to the hash extracted from the Blockchain
8. If the hashes match it means that the file has not been tampered with.
    a. If the hashes don't match it means that the file has been tampered with or is incomplete.
9. Once the hashes have been compared to each other, Software 2 creates a transaction containing the random secret (previously received from Software 1) and sends a transaction (signed with its private) to the blockchain.
10. The SFTP server of Software 2 will send the results of the compared hashes (approved/declines) and Transaction Hash of the random secret stored on the blockchain.
11. Once the SFTP receives the message Software 1 (A notification will pop-up and) it will look at the Transaction Hash and retrieve the Random Secret.
12. The Random secret sent earlier will be compared to the random secret that has been found on the Blockchain.
13. If this matched Software 1 knows that Software 2 has received the correct file and that any tampering has occurred..



1 Dia: intro
There are many security risks involved when you are sending a confidential file over the internet.

We are solving these problems!

2 Dia: architecture
We created a solution that is interoperable with the existing file transfering systems and added an extra layer of verification and security on top.
The solution provides a way to deliver files between entities in an easy, fast, secure and verifiable reliable way.
This is done by using a distributed ledger to ensure that the files received are genuine and not tempered with.
And best of all, it's easy to use.

3 Dia: login
Let’s start, first you need to login using your created username and password.

4 Dia: send files
Select the files you want to send, our solution is compatible with multiple media types such as images, video and documents.

5 Dia send files
-

6 Dia select person
Select the person you want to send the files to and press the send button. This initiates the sending process.

In the background a connection is created with your file sharing server like SFTP and the receiving SFTP server.
The Hash is derived from each individual file and a transaction with all the derived hashes is sent to the distributed ledger.

After that a package is created containing all the files, transaction hashes and a random number.
This package is sent to the receiving SFTP server.

At “Received Files” on the menu bar shows that 2 new files have been sent to you.

7 Dia Received Files

The “Received Files” shows information about the files that have been sent to you. Once the file has been received the sender receives a notification and can verify if you have received the files.

The solution automatically checks the integrity of the file. The integrity verifies if the received file has not been tampered with.

This is all done in the background, the received file is hashed and it compared against the hash that the sender has stored in the blockchain.
If this hashes match it means that the file has not been tampered with. If this hashes don't match it means that the file has been tampered with.

The receiving party lets the sender know if it received the untampered or tampered files by creating a transaction with the received random number and sending it to the distributed ledger.
After that a message is sent to the sender's SFTP server with the transaction hash of the posted random number.
The sender can fetch the saved random number and compare it to the random number that is stored on the blockchain.

End:
And that is how secure file delivery is done.