# Cloud backup 2.0: A Look Inside

Smart wallets have been growing in popularity over the past few months, in part due to their increased security advantages over traditional crypto wallets. When most people think about smart wallets, they are typically referring to wallets with a social recovery function, which eliminates the need to remember or store the seed phrase or mnemonic words.

If a user forgets the seed phrase for their traditional EOA wallet, they will be unable to regain access to their wallet, meaning the funds could be lost forever. Alternatively, if a user loses or breaks their mobile device with a smart wallet app installed, they can still regain control and recover their wallet.. This is possible through the innovative social recovery function that is native to the smart wallet. Through the use of their personalized guardians, the user can always rely on this feature to restore the smart wallet and its funds in the event that something bad happens to their device.

Smart wallets with social recovery provide users with a giant improvement in security over traditional crypto wallets by removing the single point of failure and providing this backup protection. However, this comes with a cost. As the social recovery process occurs on-chain, it involves gas costs on the Ethereum network. Due to the potential for fees to fluctuate and become expensive during periods of high demand, we have made the decision to offer users a cost-free backup source for their smart wallets. This additional feature not only provides peace of mind but also ensures that users can securely manage their wallets without any financial burden. By successfully enabling cloud backup, a user can now also rely on this function to restore the smart wallet in the case that something bad happens to the device.

We have recently completed a significant revamp of our cloud backup feature. In the following sections, we will provide a comprehensive explanation of the underlying mechanisms to help users gain a thorough understanding of how this cloud feature operates. Additionally, we will discuss the potential risks associated with its usage.

**How smart wallets work**

A smart wallet by nature is a smart contract deployed on EVM-compatible networks. This means it’s not like a traditional EOA wallet that is bound to a specific key phrase (private key). Instead, there is an owner wallet, which is then used to initiate all the transactions on behalf of the smart contract. The owner itself is an EOA address, and thus has a unique private key associated with it. Usually this private key is stored securely in the local storage of the device in which the smart wallet is installed.

The reason why the user needs to back up the key phrase of the EOA wallet is that this key phrase is directly bound to this EOA wallet. Anyone who knows this key phrase can operate this EOA wallet directly. If this key is lost, no one will be able to access the assets of this wallet anymore.

On the other hand, a user doesn’t need to back up the key phrase of the smart wallet because there is no unique private key that is directly associated with it. The owner of the smart wallet can be changed from one wallet address to another by getting the majority of the wallet’s guardians to approve the request.

**How to restore a smart wallet via social recovery**

In the case that a user is unable to access the private key of the owner of this smart wallet, one recovery approach is to change the owner of the smart wallet via the smart contract. According to the predefined logic of social recovery, after receiving majority approval from the guardians, a new wallet address will be generated and assigned as the new owner of this smart contract. With this newly generated private key of the new owner, the user is then able to regain control of the smart wallet.

Since the address of the smart wallet remains unchanged during this process, everything is now back to normal and the wallet is functional again. The only cost is the Ethereum gas fee, which the user has to pay to complete this social recovery operation as it invokes an on-chain blockchain operation.

**How to restore a smart wallet via cloud recovery**

As mentioned above, certain users may opt to bypass on-chain operations when it comes to recovering their smart wallets. This is why we’ve introduced the cloud backup and recovery option in Loopring Smart Wallet.

Cloud backup involves encrypting and storing the private key of the current owner of the smart wallet to the cloud. Considering the owner of the smart wallet may change at some point, it is necessary to back up the private key of the latest owner of the smart wallet upon detecting the owner’s change.

For cloud recovery, the process involves retrieving the private key of the owner of the smart wallet to the local device, and then restoring this EOA wallet with the key. Since the EOA wallet is set as the owner of the smart wallet, it makes it possible to fully recover this smart wallet via the cloud.

As can be seen, this approach is completely different from social recovery. In the case of social recovery, the owner of the smart wallet is changed to a new one via guardians; whereas in the case of cloud recovery, the owner of the smart wallet remains the same.

**How to implement enhanced security protection for cloud backup**

Now comes the hard part — how to ensure the security of the Cloud backup/restoration? Here is how we design and implement it for the Loopring Smart Wallet.

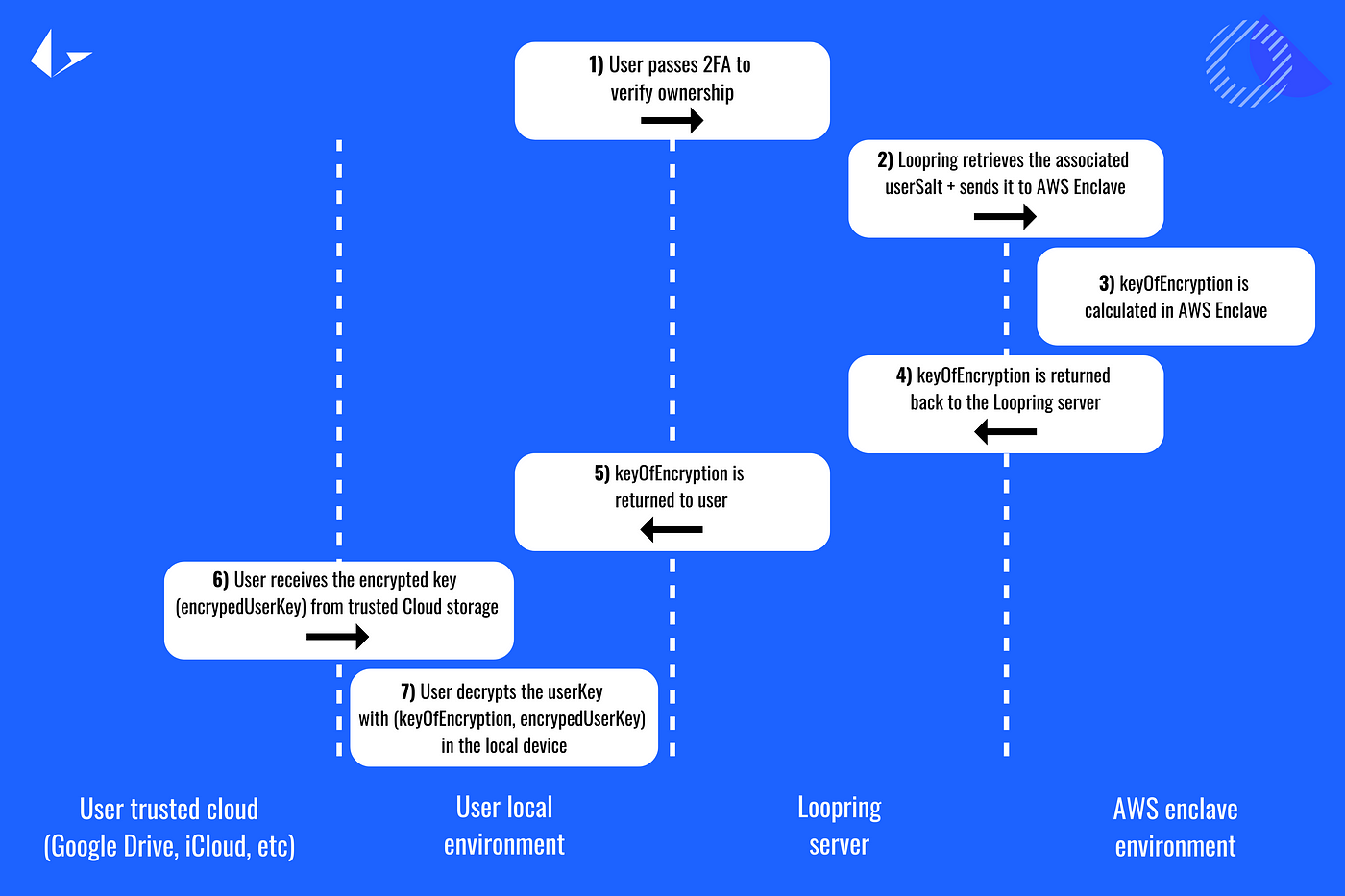
Before we get started, let’s introduce several key terms:



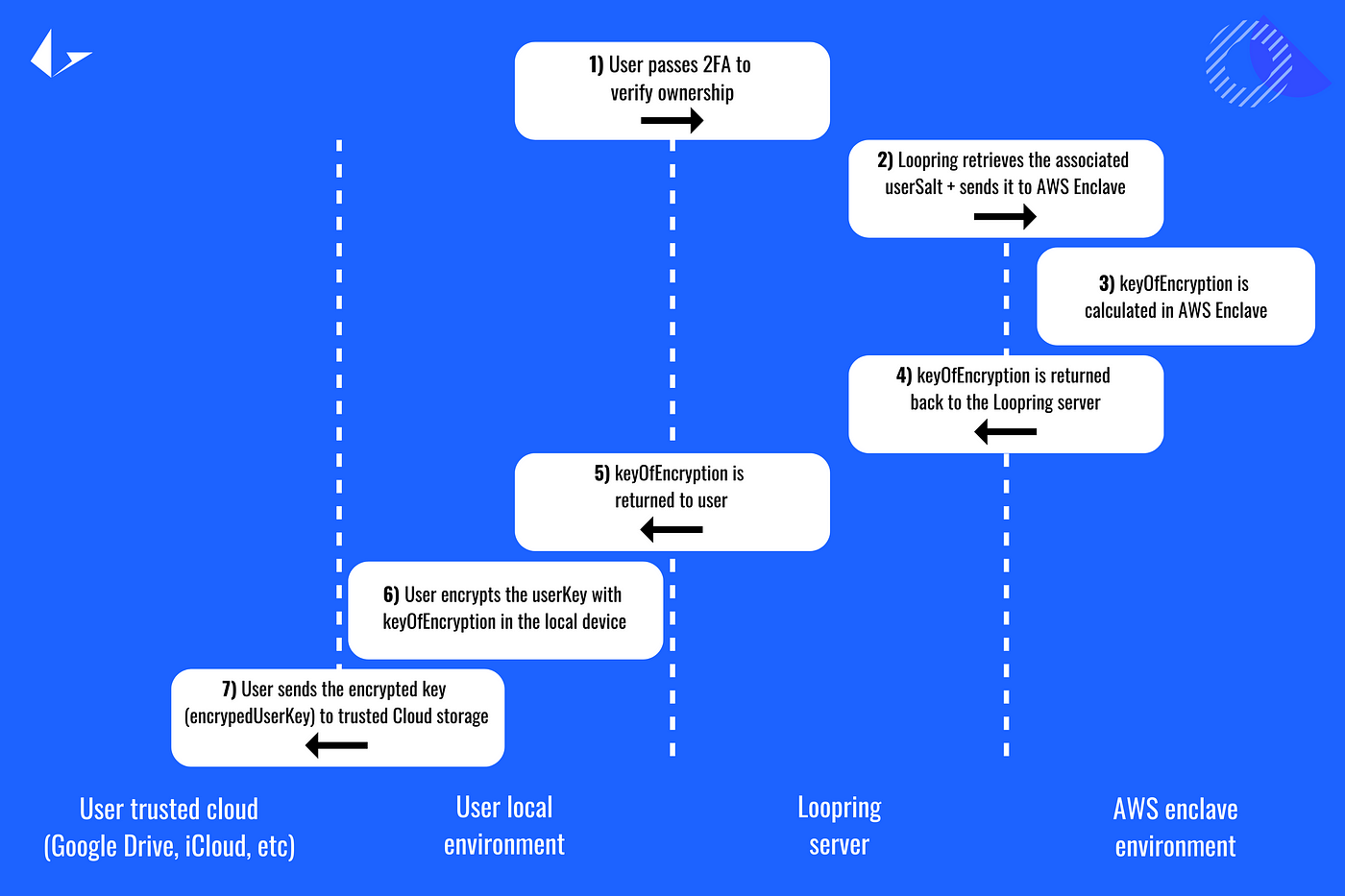
**Preparation**

The enclaveRootKey is first created by Loopring and held by selected key members. It is used to set up an AWS enclave trusted environment, which then enables Loopring to create isolated compute environments to further protect and securely process highly sensitive data. Then, for each smart wallet, the corresponding userSalt is generated in the Loopring server and stored there.

**Backup**

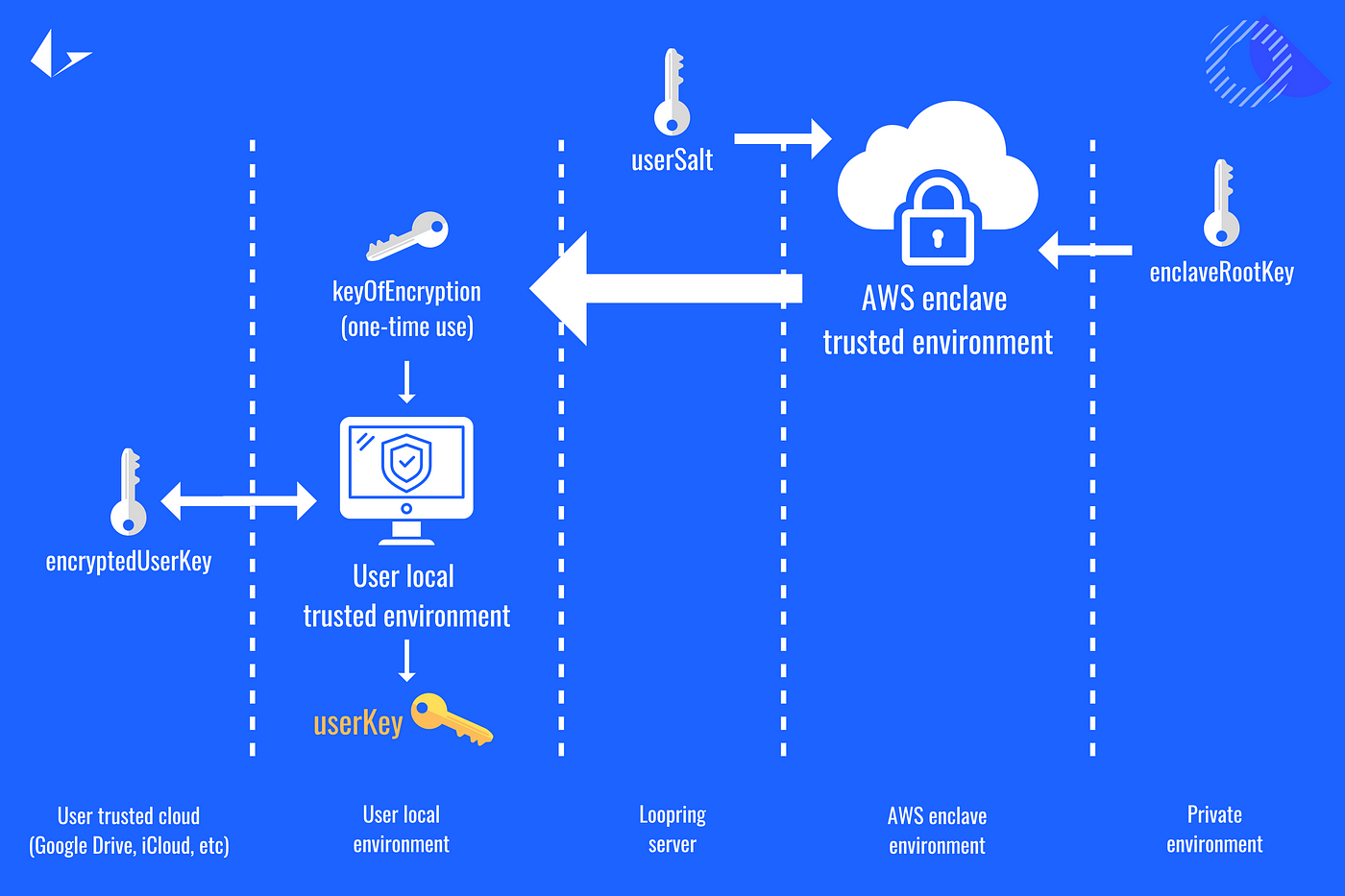
Below you can see a full flow of the step-by-step operations that are invoked during the backup process. The backup is completed when the encrypted user key is uploaded to the user’s personal cloud storage.

**Restoration**

Below you can see a full flow of the step-by-step operations that are invoked during the restoration process. After the user decrypts the encryptedUserKey to properly restore the userKey, they are able to regain control of the owner wallet, which is then able to fully control the smart wallet once again.

**Key isolation**

As seen below, there are 5 environments involved in cloud backup and recovery:

1. Loopring private environment
2. AWS isolated enclave environment
3. Loopring server
4. User local environment
5. User trusted cloud storage
6. The enclaveRootKey is maintained by Loopring core members in the private environment. With the enclaveRootKey, the isolated enclave environment can be established in AWS. The enclave environment doesn’t store any keys; it is only a runtime environment for trusted computation.
7. The userSalt is stored in the Loopring server, which is used to calculate the corresponding keyOfEncryption in the AWS enclave environment.
8. The userKey is stored in the user’s local environment for normal smart wallet usage.
9. The encrypted user key (also known as the encryptedUserKey) is stored in the user’s trusted cloud storage.
10. The keyOfEncryption will not be saved in either part; instead, it’s dynamically computed and returned to the user for temporary usage and is discarded after usage.

The only two keys that could be exposed to malicious hackers are the encryptedUserKey, which is stored in the user’s trusted cloud storage (Google Drive or Apple iCloud) and the userSalt, which is stored in the Loopring server. However, even if a hacker manages to get the encrypted key, they are still unable to decrypt it without knowing the keyOfEncryption. On top of this, even if a malicious hacker exploits the Loopring server and obtains the userSalt, they would be unable to generate the real keyOfEncryption as the AWS enclave environment remains secure. By removing any single point of failure, we are confident our cloud backup and recovery feature will be a robust and secure option for many users.