CryptoTestament: a smart contract solution for testaments

LiberDApps
liberdapps@protonmail.com

Abstract. In this paper, we propose an approach for creating crypto testaments where funds can be transferred to a beneficiary after the testator dies. By leveraging smart contract based blockchains, the proposed system can work in fraud-proof environments that eliminate the need for trusted third-parties, lawyers, executors, judicial processes, and other factors that may prevent a testament from being honored.

Dealing with crypto legacy

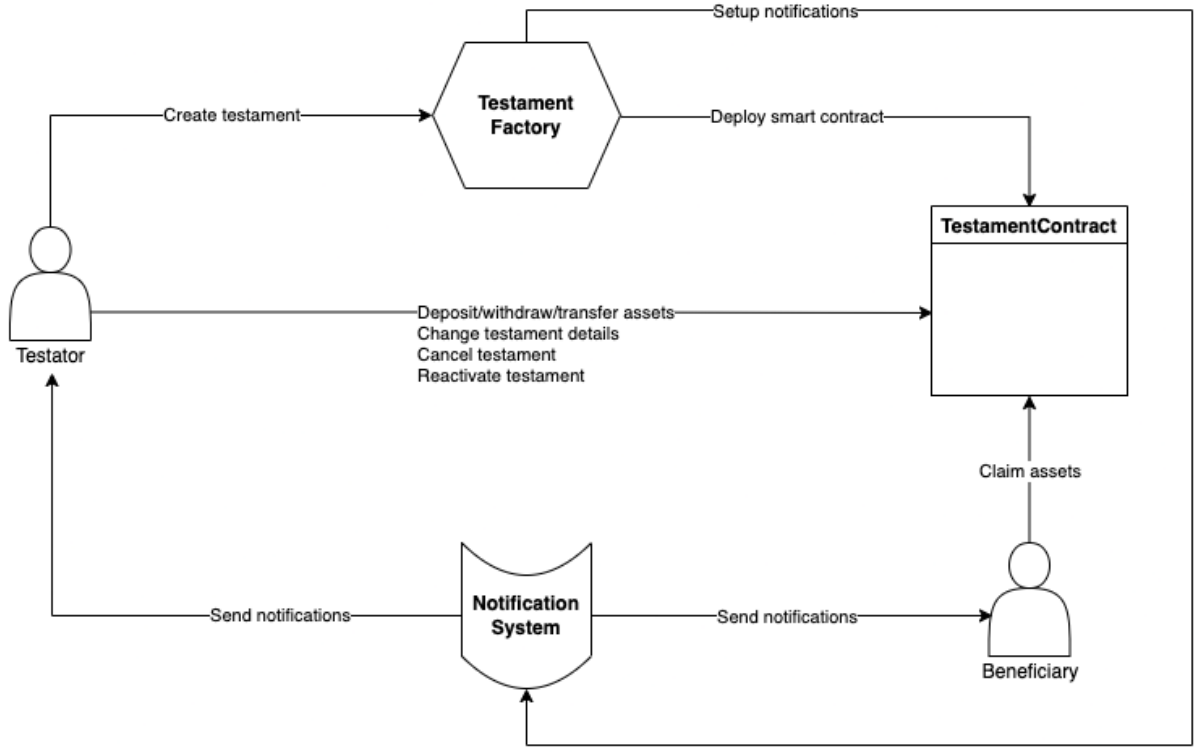
In the crypto world, there's a famous saying that goes: "Not your keys, not your coins.''. That simply means that if you don't have access to the private keys for the wallet that controls your coins, they aren't yours. This is especially true when users keep their funds in centralized exchanges: while this is the most convenient option, it is far from the safest, as exchanges are frequently hacked, go out of business, or freeze funds for other reasons. Unfortunately, many people had to learn that lesson the hard way. The alternative is self-custoding your crypto, which means you are responsible for carefully holding your assets, keeping hackers away, and putting up backups and recovery plans. Users have a variety of alternatives in this regard, ranging from simple mobile apps to more complex settings such as hardware wallets protected by pin codes and passphrases.

Although there are numerous methods for safely storing cryptocurrencies, one topic that we don't see much debate about is what happens to your crypto after you pass away. Traditionally, a testamentary trust[1] can be established, which is a legal arrangement in which the testator – the person who establishes the trust – appoints a trustee – a trusted third-party – to safeguard the testator's assets until the beneficiaries can take possession of them. Testators are free to move the funds and amend the testament conditions while they are still alive. When the testator dies, the legal relationship begins, and it is governed by the testator's last will, which specifies how and under what conditions the assets should be distributed. The entire process can be time-consuming, requires probate[2], and is subject to taxation and other considerations that may cause the testator's last will to be partially or completely disregarded. When crypto is concerned, another drawback of the traditional approach is that it would require testators to disclose their private keys to third-parties and, as mentioned, that's a big security risk. Luckily, new possibilities have surged in the crypto days, and we'll go over a potential solution for overcoming such challenges.

Smart contracts as an alternative solution for testaments

Smart contracts allow us to define rules that can be enforced in a predictable and automated way, resulting in immutable and self-executing agreements. This can greatly reduce, if not completely eliminate, the need for trust and subjectivity in human decision-making, opening up new methods of dealing with testaments.
Using smart contract-based blockchains, such as the *Ethereum*[3] blockchain, we can build a platform where anybody may create a testament contract in which assets are transferred to a beneficiary under certain conditions, without any need for trustees, executors, or court processes.

The diagram below shows how such a system can be constructed:



1. Testators create testaments contracts through a factory component.
2. The testament contract functions as a smart wallet for which only the testator has the private keys, allowing funds to be safely deposited, withdrawn and transferred from the contract.
3. The contract also allows a beneficiary, as defined by the testator, to claim the funds available after the testator's death.
4. For the benefit of both the testator and the beneficiary, a notification system is in place to alert them to events related to the testament.

Testators should be able to freely move funds stored in the testament contract as long as they are alive, and these funds should remain inaccessible (locked) to beneficiaries during that time. The funds held in the contract can be claimed by the beneficiaries after the testators have passed away.

To be transparent, fraud-proof, and immutable, all logic and data used by smart contracts should be available on the blockchain, however death is a real-world event that occurs outside of the blockchain. If death events were recorded in decentralized and trustless networks, we could leverage oracles to reliably determine when a testator dies, but this isn't currently possible. Alternatively, we can use a proof of life as a workaround for the lack of oracles. A proof of life is an action that testators must take within a particular time frame to demonstrate that they are still alive and in control of their assets, i.e., a clear signal that they are not dead and that their testaments should remain locked. If testators do not provide proof of life after a certain period of time, the smart contract will assume they are no longer alive and will allow beneficiaries to claim the available funds held in the contract.

Creating testaments

When creating a testament, a testator should provide the following details:

* Testator name
* Testator email
* Beneficiary name
* Beneficiary email
* Beneficiary wallet address
* Proof of life threshold

The names and emails will only be used by the notification system, and they should be encrypted before being published on a public blockchain. The notification system serves as a facilitator, keeping track of events related to the testament and contacting the testator or beneficiary as needed. After the testator dies, the beneficiary may claim the funds stored in the testament contract by using the wallet address specified by the testator while creating the testament. Finally, the proof of life threshold is the number of months in which the testator is required to send a proof of life on a regular basis. For example, if the testator sets this threshold at 3, the testator must send proof of life every three months to keep the testament contract locked.

Providing a proof of life

After creating a testament contract, the testator will be able to use it as a wallet, freely depositing, withdrawing, and transferring funds in the contract. All of these actions constitute proof of life since they clearly indicate that the testator is actively using the funds and that the testament should remain locked. Testators can also send a proof of life by changing any detail (names, emails, beneficiary address, or the threshold for the proof of life).

The testament contract will keep a timestamp of when the last proof of life was sent, and the notification system will use that timestamp to remind testators when it is time to send another proof of life.

Canceling and reactivating testaments

If the beneficiary has not yet claimed the funds in a testament contract, the testator has the option to cancel it. When a testament is cancelled:

1. The beneficiary is no longer able to claim the funds in the testament.
2. The notification system will no longer send any messages.
3. The testator can still move the funds in the testament contract at any time.

The testator can also use a function in the testament contract to reactivate a previously cancelled testament. When a testament is reactivated:

1. The timestamp of the most recent proof of life is updated..
2. When the testator stops providing proof of life, the beneficiary will be allowed to claim the funds in the testament.
3. Notifications will be sent again by the system.

Claiming funds in a testament contract

If testators do not provide proof of life within a certain period, their beneficiaries will be allowed to claim the funds in their testament contracts. The notification system should monitor and notify the beneficiaries of these events, assisting them in collecting their rightfully owned crypto legacy. It's worth noting that only the beneficiary should be able to claim the funds in the testament contract by utilizing the wallet address specified by the testator in the contract, and the smart contract will ensure that's the case.

Final considerations

In this paper, we presented a solution that, with the help of smart contracts, can offer an alternative for people who want to leave a crypto legacy without having to rely on a third-party to custody and transfer the assets. The strategy may be implemented on a variety of smart contract platforms, with differing degrees of decentralization, speed, transaction costs, and resilience to censorship. Furthermore, because these blockchains often include tokenized assets (such as stablecoins, derivatives and NFTs), the system may be able to support these tokens with ease, enhancing the user experience and asset coverage.

Finally, the platform may be directly connected with wallets, giving users the ability to not only self-custody their crypto assets, but also to choose who inherits their crypto legacy when they die.

References

[1] *Testamentary Trust* - https://www.investopedia.com/terms/t/testamentarytrust.asp
[2] *Probate* - https://legal-dictionary.thefreedictionary.com/probate
[3] *Ethereum* - *https://ethereum.org*