Will-wallet: A **Peer-to-Peer** Trustless custodian solution.

Yilak kidane
yilakb@lbtil.com
www.will-wallet.com
12-1-2018

Abstract: Bitcoin protected by unbreakable cryptography. This attribute makes it a secure way to store wealth, but also creates the risk that when Bitcoin owner pass without passing on the private key, his heirs may discover his wallet only to realize that they will never gain access to the wealth inside. To prevent this, the owner must ensure someone gets a copy of the private key or entrusting it with a commercial service that manages them. Some of these methods come with their own perils and difficult to rely on.

Anyone can address these issues by simply following this simple step. The example in this paper demonstrates how to safely transfer bitcoin to the rightful heirs without relying on a third party, maintain full control over your bitcoin, and make any necessary changes without worrying about losing bitcoin or incurring extra expenses.

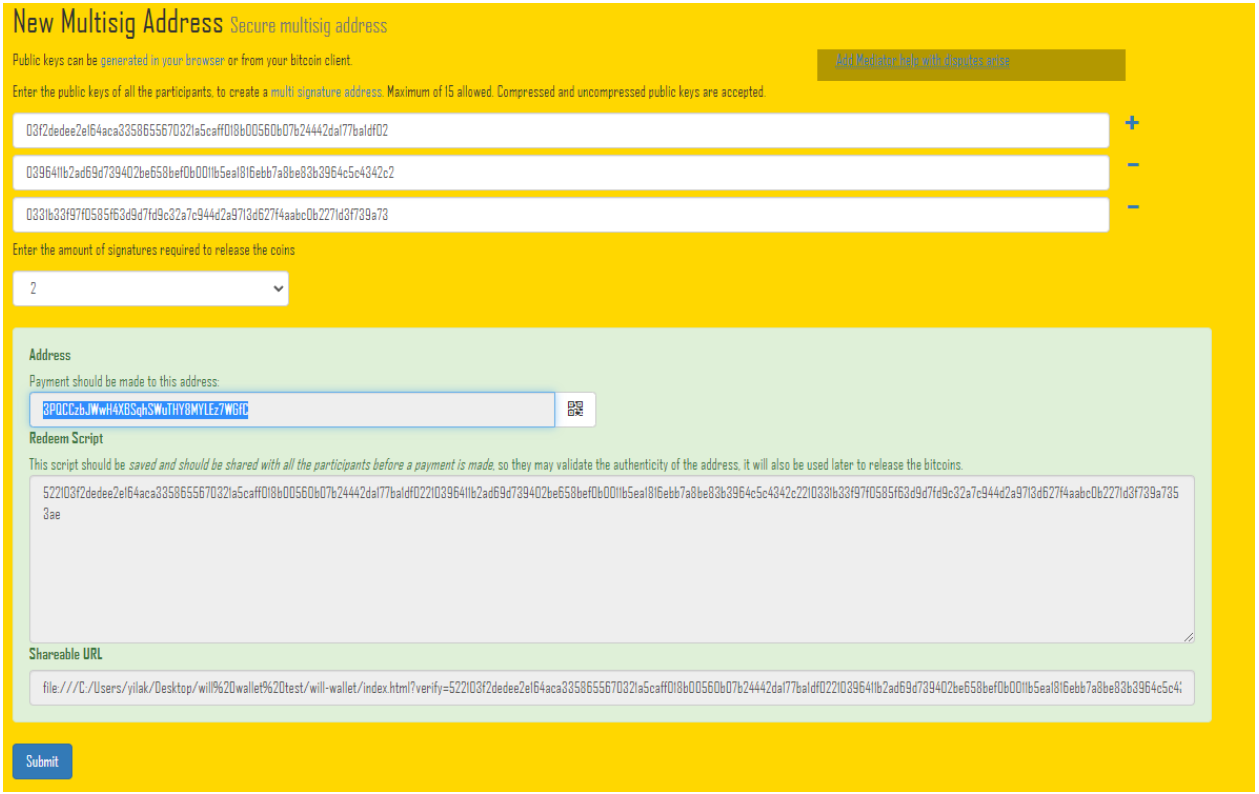
This are wallet crated to show the steps. wallet

1st Will sender address SegWit Address bc1q6urj690j7kc0nnnf2tgell0za6fndlwu8z7h53 RedeemScript d7072d15f2f5b0f9ce6952d19ffde2ee9336fddc Public key 03f2dedee2e164aca3358655670321a5caff018b00560b07b24442da177ba1df02 Private key (WIF key) L2XUVL1adnCuTkykcFCxN9ARvjkMj1ffXB5Q6m6nEQfce6r9Sg2J
2nd will sender address s SegWit Address bc1q3rp9d0af0w6f2ax4hadhe6y3m2r49lwwr8uwt2 RedeemScript 88c256bfa97bb49574d5bf5b7ce891da8752fdce Public key 0396411b2ad69d739402be658bef0b0011b5ea1816ebb7a8be83b3964c5c4342c2 Private key (WIF key) KyDD8zXt9RbR8YagSUSddBtNW5FjYoTPFFxhx4g5pTKqc9jFfcdU
Will receiver address (For practical, real-world application receiver only need to provide public key) SegWit Address bc1qqhkqj8yxn5fw4t6kv3s966a03xvhljzaqf0qxr RedeemScript 05ec091c869d12eaaf5664605d6baf89997fc85d Public key 0331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a73 Private key (WIF key) L2Mcu3NJubh8gRQ5PTewqPsXGrjf5eCRx8m8KACr3DhdvwCspSFs

Step 1 [Create Multisig Address]

Create a multi signature address using (will receiver public key and will sender 1st& 2nd public key.)

Creating a (2, 3) Multisig address gives you control over two private keys, which are necessary to make changes if needed. When you are setting up the inheritance transfer to happen at a specific date in the future, you have full control over the funds during that time and can adjust the recipient or sign it over to someone else if necessary.



New Multisig Address: 3PQCCzbJWwH4XBSqhSWuTHY8MYLEz7WGfC

Redeem Script

522103f2dedee2ef64aca3358655670321a5caff018b00560b07b24442daf77ba1df02210396411b2ad69d739402be658bef0b0011b5ea1816ebb7a8be83b3964c5c4342c2210331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a7353ae

Step 2 [Allocate]

Send the desired amount of Bitcoin you would like to include in the inheritance plan to the newly created Multisig address.

For this example, 0.00008244 BTC send to this newly created Address 3PQCCzbJWwH4XBSqhSWuTHY8MYLEz7WGfC

TransactionId:[507c6437f0d17f6301e6c26ce0dcf3c5e18da869b34abf0daab99313d5e5cc3a]

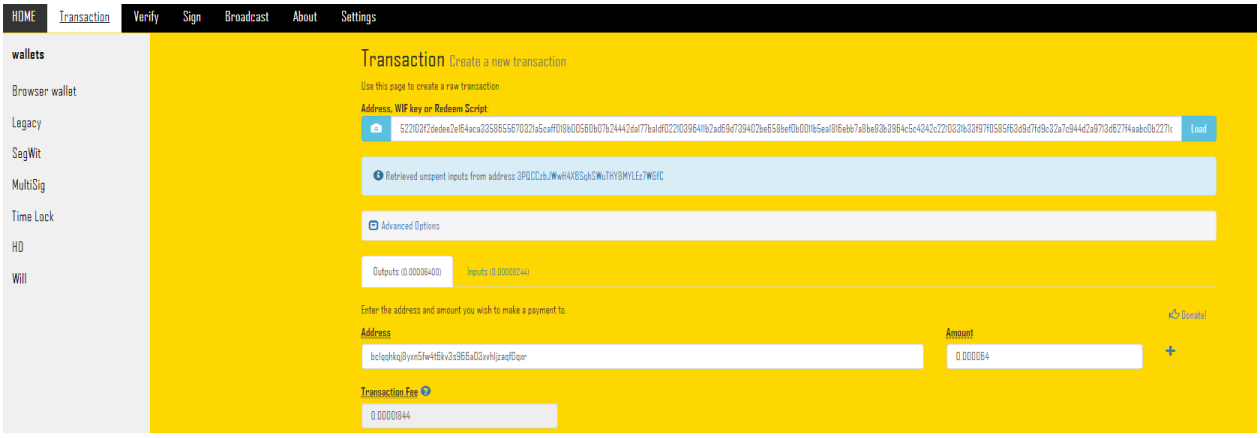
Step 3 [Create a new transaction.]

Create a transaction to the Will receiver address: bc1qqhkqj8yxn5fw4t6kv3s966a03xvhljzaqf0qxr

using the Multisig redeem script from step 1.

We can adjust in this step by including our return address or another receiver if we have more Bitcoin in the address than we would like to include in this will or if we need to send for multiple will recipients.

For this example, only one receiver gets the entire will.



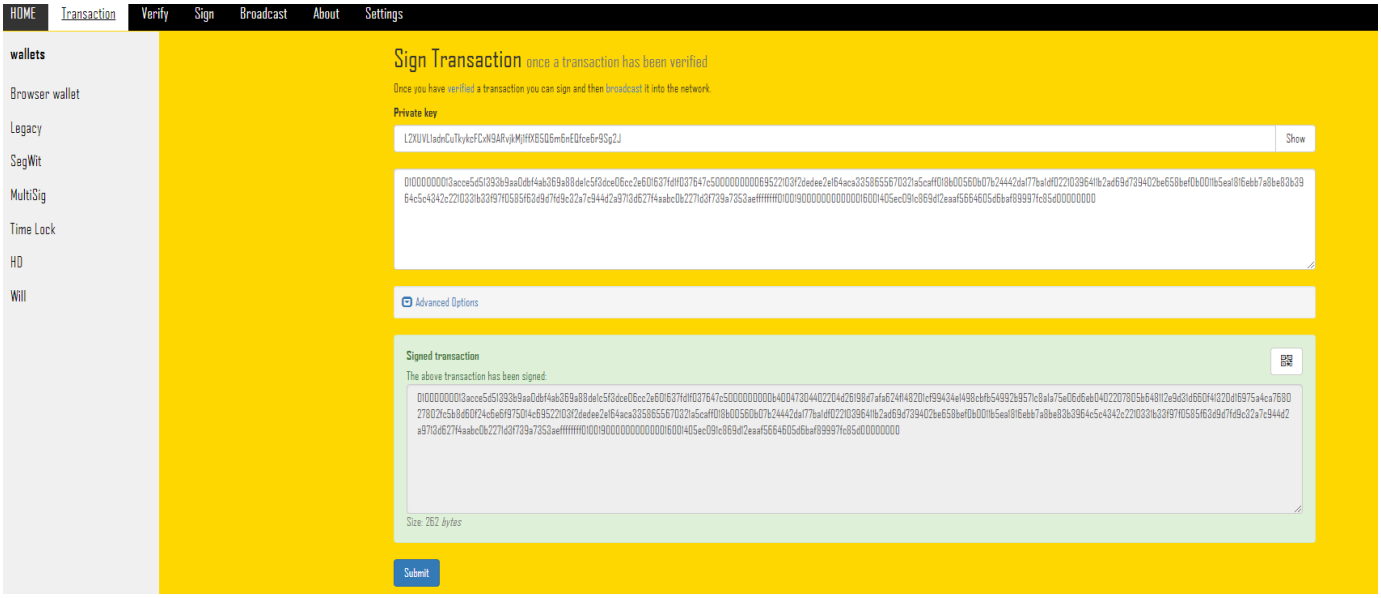
Raw transaction

01000000013acce5d51393b9aa0dbf4ab369a88de1c5f3dce06cc2e601637fd1f037647c5000000000695221 03f2dedee2e164aca3358655670321a5caff018b00560b07b24442da177ba1df02210396411b2ad69d739402be658bef0b0011b5ea1816ebb7a8be83b3964c5c4342c2210331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a7353aefffffffff0100190000000000001600 1405ec091c869d12eaaf5664605d6baf89997fc85d00000000

Step 4 [Sign transaction.]

Using 1st private key of Will sender, we sign the Raw transaction.

Private Key (WIF key): L2XUVL1adnCuTkykcFCxN9ARvjkMj1ffXB5Q6m6nEQfce6r9Sg2J



This transaction has been signed with one private key.

01000000013acce5d51393b9aa0dbf4ab369a88de1c5f3dce06cc2e601637fd1f037647c5000000000b40047304402204d26198d7afa624f148201cf99434e1498cbfb54992b9571c8a1a75e06d6eb0402207805b648112e9d31d660f41320d16975a4ca768027802fc5b8d60f24c6e6f975014c69522103f2dedee2e164aca3358655670321a5caff018b00560b07b24442da177ba1df02210396411b2ad69d739402be658bef0b0011b5ea1816ebb7a8be83b3964c5c4342c2210331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a7353aeffffffff0100190000000000000160014405ec091c869d12eaaf5664605d6baf89997fc85d00000000

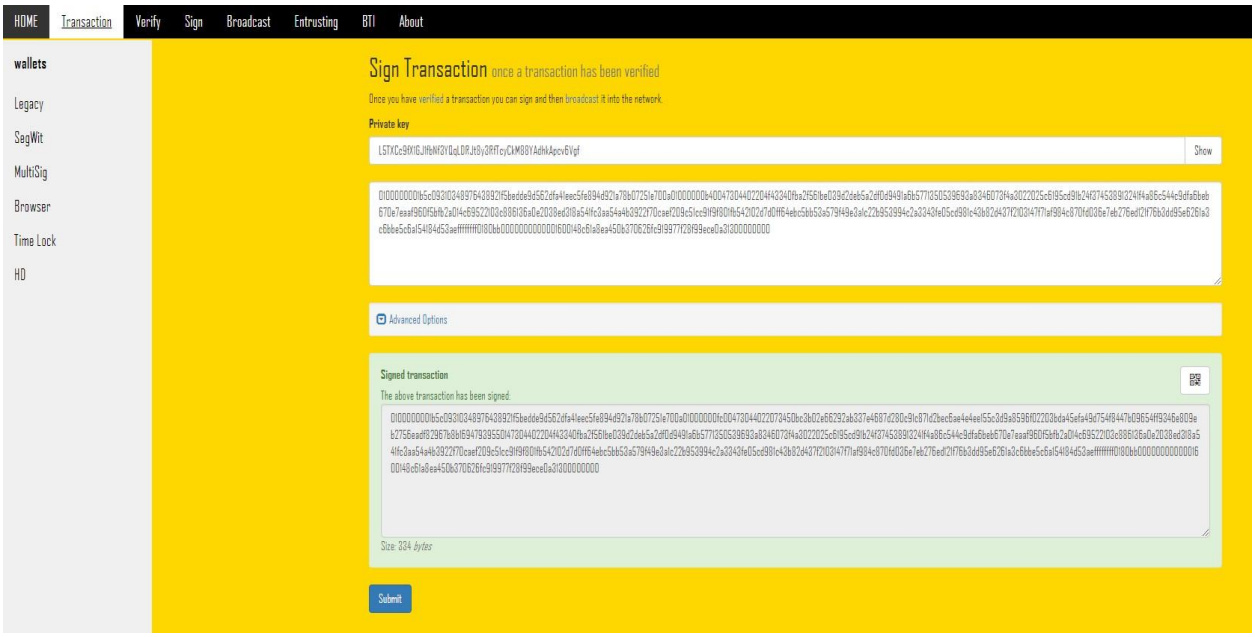
Step 5 Arrange delivery.

Arrange for a future delivery of the half-signed transaction to the intended recipient through a delayed text message, email, or estate planner in a specific future date or circumstance.

The use of a third party is entirely up to your discretion and only takes place after the contract has been enforced, ensuring the safety of the bitcoin even if the half signed raw transaction is held by or made public by a third party.

The half-signed raw transaction can only be executed with one of the two remaining private keys, one held by the recipient(will-receive) and the other held by the sender(you).

Once the inheritance recipient receives the half-signed raw transaction, they can sign it with their private key and broadcast it to receive the digital asset in their wallet.



Fully Signed transaction ready to be broadcast.

1st signed by one of the sender privet keys.
2nd signed by will receiver privet key.

01000000013acce5d51393b9aa0dbf4ab369a88de1c5f3dce06cc2e601637fd1f037647c5000000000fdfd000047304402204d26198d7afa624f148201cf99434e1498cbfb54992b9571c8a1a75e06d6eb0402207805b648112e9d31d660f41320d16975a4ca768027802fc5b8d60f24c6e6f97501483045022100b79888e797dbcf18701ec20897a989d307a70ca9c59d56756ad533ed51d295e0022030c02fecb28793e5444121e867dd4bc5c08e08ba79dca356c2c17ca5fce0e8d0014c69522103f2dedee2e164aca3358655670321a5caff018b00560b07b24442da177ba1df02210396411b2ad69d739402be658bef0b0011b5ea1816ebb7a8be83b3964c5c4342c2210331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a7353aeffffffff0100190000000000001600140 5ec091c869d12eaaf5664605d6baf89997fc85d00000000

Step 6 Broadcast.

txid: a0656892a46ea36ac2285292calea388837f6793b35848e0b6ca625d4e4f6ea5

Once the transaction is confirmed on the Bitcoin blockchain, the inheritance recipient will receive the Bitcoin in their wallet.

Time lock Option

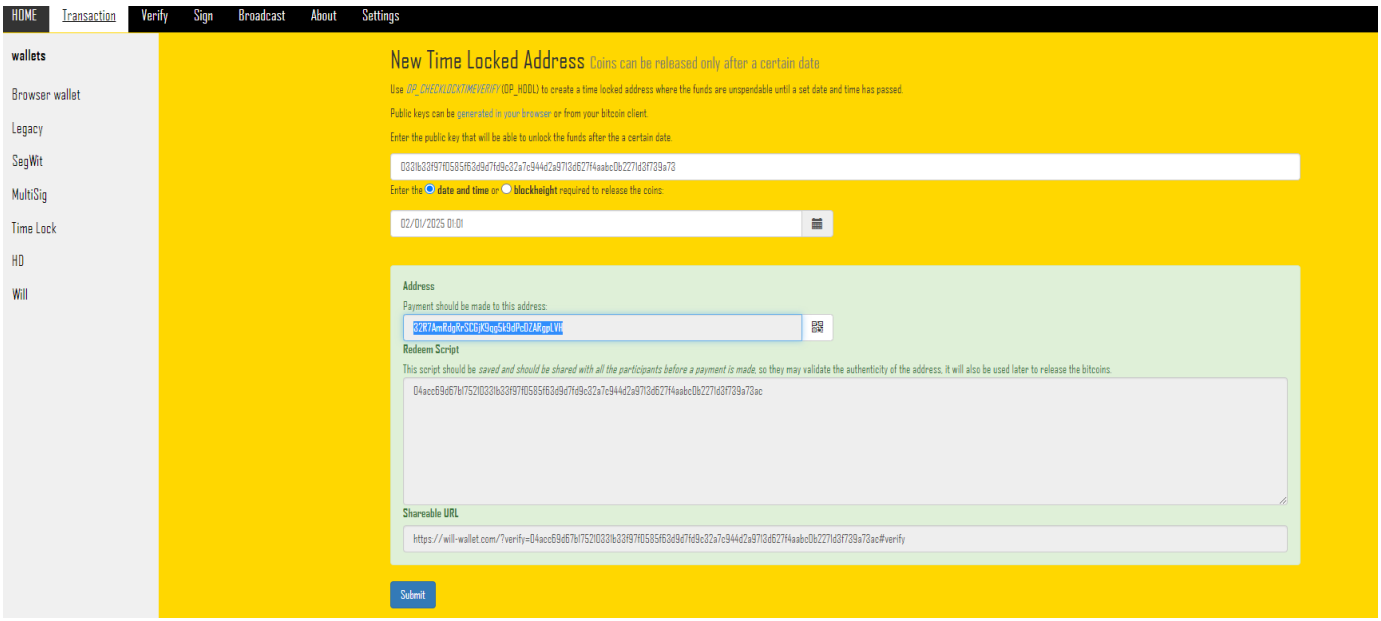
A time lock can be added to ensure that the Bitcoin is not accessible before the intended time, allowing for the raw transaction to be delivered to the recipient without the need for a third-party messaging system.

Include Step 2.5

Create New Time Locked Addresses from the Will receiver's public keys, and the bitcoin can only be released after the date or blockheight the sender set.

To create a time locked address where the funds can't be spent until a set date and time has passed.

Public key of receiver: 0331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a73



Fund release date set by sender 02/01/2025 01:01 and transaction should be made to this receiver

address: 32R7AmRdgRrSCGjK9qg5k9dPcDZARgpLVH

Redeem Script

This script should be saved and should be shared with all the participants before a payment is made, so they may validate the authenticity of the address, it will also be used later to release the bitcoins.

04acc69d67b175210331b33f97f0585f63d9d7fd9c32a7c944d2a9713d627f4aabc0b2271d3f739a73ac

continue the same process from Step 3.

This method Provide versatility, security, and flexibility without 3rd party trust.

1. The sender has the ability to release the Bitcoin at any time before the recipient signs the transaction, and if circumstances change, the transaction can be re-signed to a different receiving address with the two private keys held by the sender.

2. For those who wish to divide their assets among multiple recipients, multiple wallet addresses can be included in step 3. Only one recipient is required to sign the second signature and broadcast the transaction, and all recipients will receive the funds simultaneously in their personal wallets.

3. If the transaction fee set when the transaction is constructed is not enough at the time of broadcasting a fully Signed transaction, the receiver has the option to do either RBF (Replace by Fee) or CPFP (Child Pays for Parent).

4. The sender will be considered to have sent the transaction at the price when he signs the first signature on the transaction, and the receiver will also be considered to have received it at whatever time price when he signs to receive the bitcoin, this fact can reduce the tax liability for both parties. (I'm not a tax lawyer, the last point is just based on assumptions.)

Conclusion

If set up in advance, this could be a solution for transferring ownership of Bitcoin in the unfortunate event of the owner's passing or for any other circumstances that prevent the holder from transferring their asset. This method's application is not restricted to the use case above; it can also be used in exchanges, monthly payout trust funds, insurance payouts, and estate transfers, among other custodian solutions.

Yilak b kidane
Email: yilakb@lbtil.com
Twitter: https://twitter.com/yilakb