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.

Will-wallet: Aiming to solve problems we encounter when it comes to digital asset custody. The solution proposed in this paper improve your digital assets to be transferred safely to the rightful heirs without trusting 3nd party and enables you to maintain full Control of your fund, make some changes if necessary, without any concern of losing asset or bear unnecessary costs.

The following example below illustrates, how this can be achieved by using will-wallet on Bitcoin network.

Create address: http://will-wallet.com/#newAddress

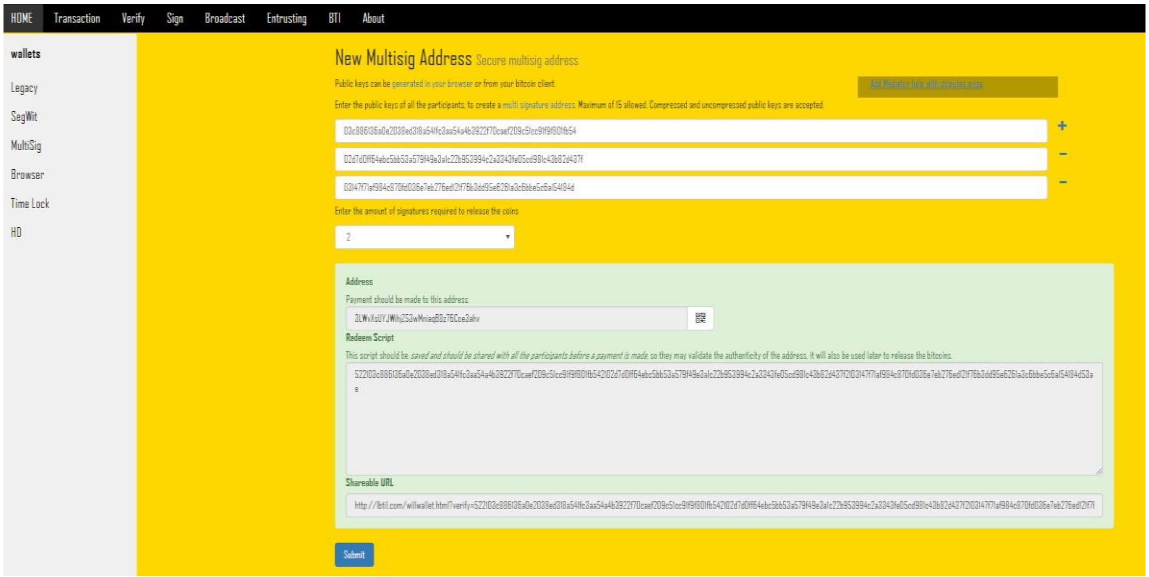
1st Will sender address Address bc1qdg6z5ulq036k7f6jkfzup6addvpna0qlaxsz5h Redeem Script 6a342a73e07c756f2752b245c0ebad6b033ebc1f Address Public key 02d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f Private key L4S2cgu1YjUP7M1F87wG6kjUyCXtJvXAsNqNNrncR7qeqWpdNSM2
2nd will sender address (optional but recommended) Address bc1qceq6s66e3f7emydcfalxur6tpdvdzkxl7hskwn Redeem Script c641a86b598a7d9d91b84f7e6e0f4b0b58d158df Public key 03147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d Private key L2TktDeSDZHgeNdzqCe3xG1jZNzNA2E69nrG3XC8fbhaxxmwmRuu
Will receiver address (For practical, real-world application receiver only need to provide public key) Address bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s Redeem Script 8c61a8ea450b370626fc919977f28f99ece0a313 Public key 03c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54 Private key L5TXCc9fX1GJ1fb3YQqLDRJt8y3RfTcyCkM88YAdhkApcv6Vgf

Step 1

Create Multisig Address http://will-wallet.com#newMultiSig

Create a multi signature address using (will receiver address, 1st address Will sender, 2nd address will sender.)

Crating (2, 3) Multisig address, enables you to control the two private keys needed to make some change if necessary, after we set up the will to be transferred on a specific future date, during that time you have full control of the fund to adjust or sign it to different receiver if needed



New Multisig Address Secure multisig address

Public keys can be generated in your browser or from your bitcoin client.

Enter the public keys of all the participants, to create a multi signature address. Maximum of 15 allowed. Compressed and uncompressed public keys are accepted.

03c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54

02d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f

03147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d

Enter the amount of signatures required to release the coins

2

Address

Payment should be made to this address:

3LWvXsUYJWihjZ53wMniaqB8z76Coe3ahv

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.

```
522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53a
e
```

Shareable URL

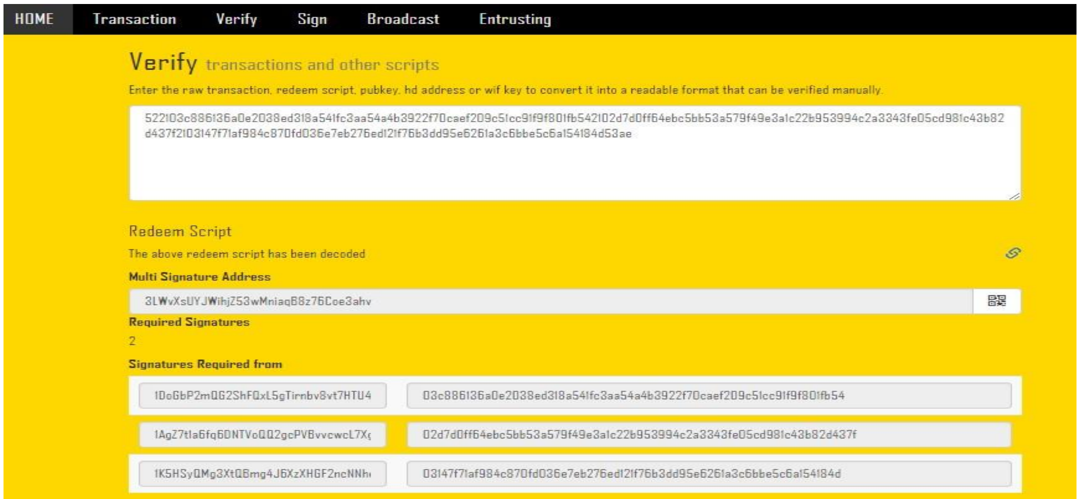
http://btil.com/willwallet.html?verify=522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f7

New Multisig Address: 3LWvXsUYJWihjZ53wMniaqB8z76Coe3ahv

Redeem Script

522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53ae

http://will-wallet.com#verify



Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82
d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53ae
```

Redeem Script

The above redeem script has been decoded

Multi Signature Address

3LWvXsUYJWihjZ53wMniaqB8z76Coe3ahv

Required Signatures

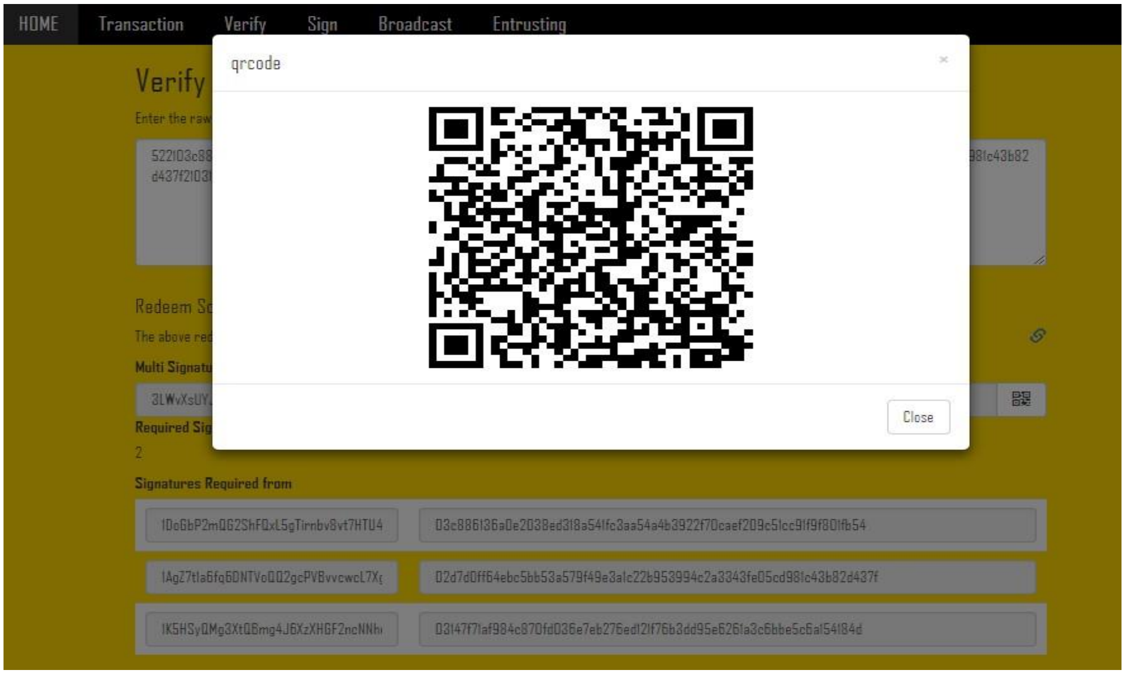
2

Signatures Required from

1DoGbP2mQG2ShFQxL5gTirnbv8vt7HTU4	03c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54
1AgZ7tla6fq6DNTVoQQ2gcPVBvvcwcL7X(	02d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f
1K5HSyQMg3XtQBmg4J6XzXHGF2ncNNh	03147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d

Step 2

Send the desired amount of digital asset like to include in the will to the newly produce Multisig address.



Verify

Enter the raw

522103c88 ... 981c43b82
d437f2103

Redeem Sc

The above red

Multi Signatu

3LWvXsUY

Required Sig

2

Signatures Required from

1DoGbP2mQG2ShFQxL5gTirnbv8vt7HTU4	03c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54
1AgZ7tla6fq6DNTVoQQ2gcPVBvvcwcL7Xg	02d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f
1K5HSyQMg3XtQ6mg4J6XzXHGF2ncNNh	03147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d

Step 3

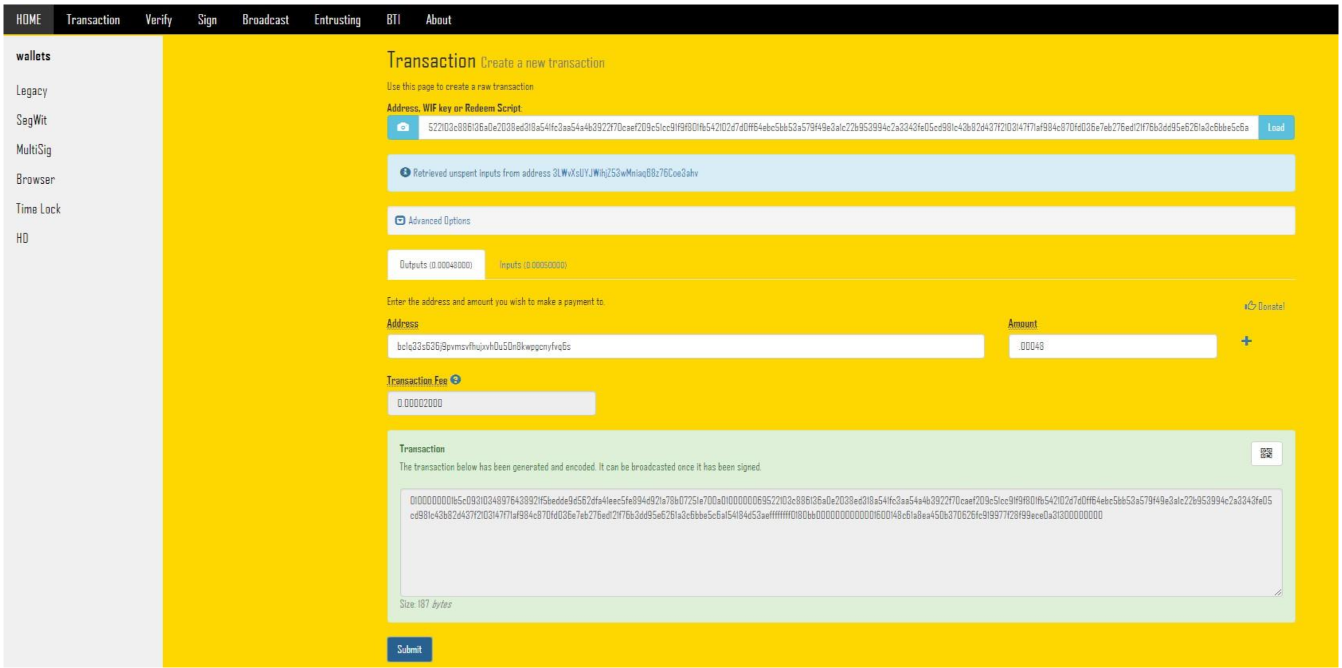
Create a new transaction: http://will-wallet.com/#newTransaction

Create a transaction to the Will receiver address:bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s

using the Multisig redeem script from step 1.

In this step, if we have more fund in the address then we like to include in this will or we need to send for several will receiver we can adjust that by including our return address or other receiver address.

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



Transaction Create a new transaction

Use this page to create a raw transaction

Address, WIF key or Redeem Script:

```
522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a
```

Retrieved unspent inputs from address 3LWvXsUYJWihjZ53wMniaqB8z76Coe3ahv

Enter the address and amount you wish to make a payment to.

Address	Amount
bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s	.00048

Transaction Fee: 0.00002000

Transaction

The transaction below has been generated and encoded. It can be broadcasted once it has been signed.

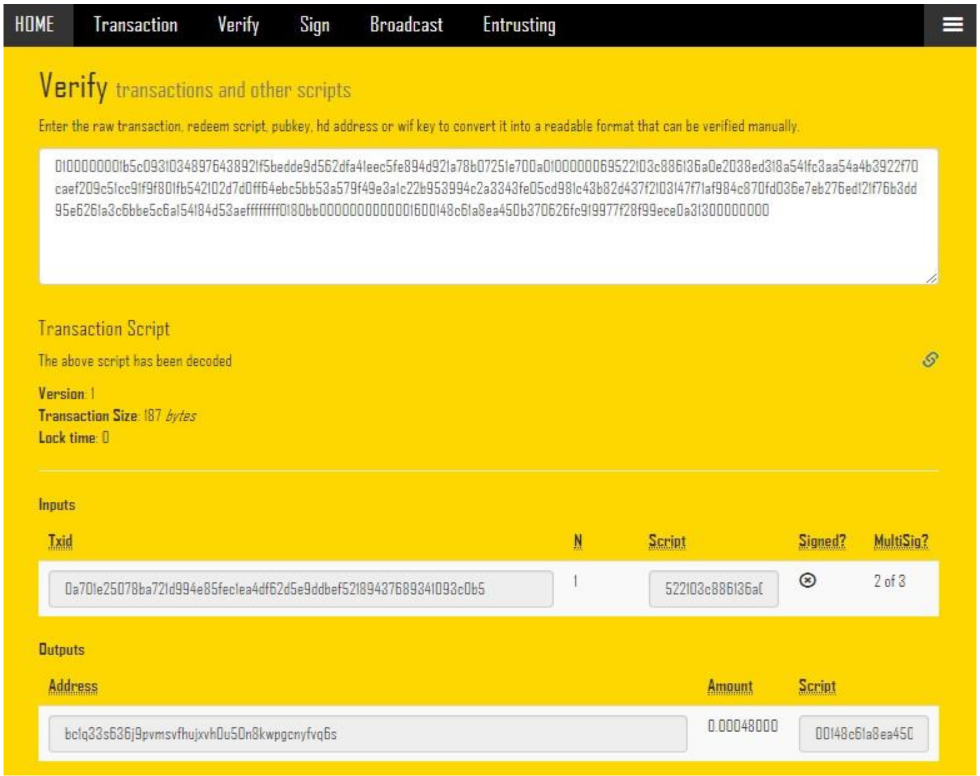
```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a0100000069522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05
cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

Size: 187 *bytes*

Raw transaction

0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a0100000069522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed 121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000

Verify



Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a0100000069522103c886136a0e2038ed318a541fc3aa54a4b3922f70
caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd
95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

Transaction Script

The above script has been decoded

Version: 1
Transaction Size: 187 *bytes*
Lock time: 0

Inputs

Txid	N	Script	Signed?	MultiSig?
0a701e25078ba721d994e85fec1ea4df62d5e9ddbef52189437689341093c0b5	1	522103c886136a(	⊗	2 of 3

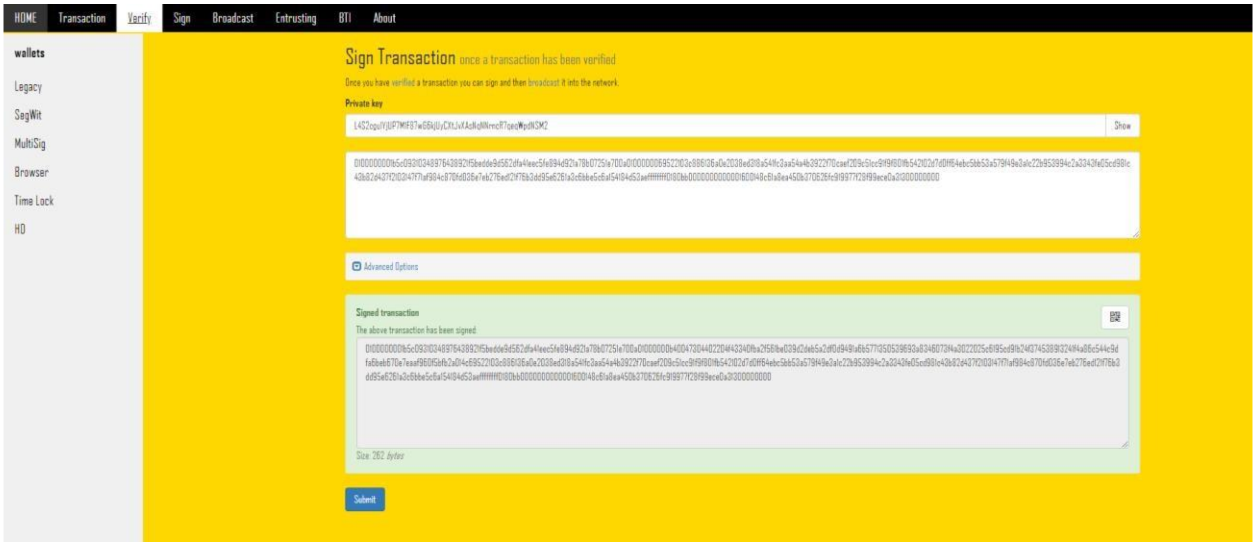
Outputs

Address	Amount	Script
bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s	0.00048000	00148c61a8ea450

Step 4
Sign transaction: http://will-wallet.com/#sign

Using 1st privet key of Will sender we sign the Raw transaction

Private Key (WIF key): L4S2cgu1YjUP7M1F87wG6kjUyCXtJvXAsNqNNrncR7qeqWpdNSM2



Sign Transaction once a transaction has been verified

Once you have verified a transaction you can sign and then broadcast it into the network.

Private key

L4S2cgu1YjUP7M1F87wG6kjUyCXtJvXAsNqNNrncR7qeqWpdNSM2 Show

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a0100000069522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c
43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

Signed transaction

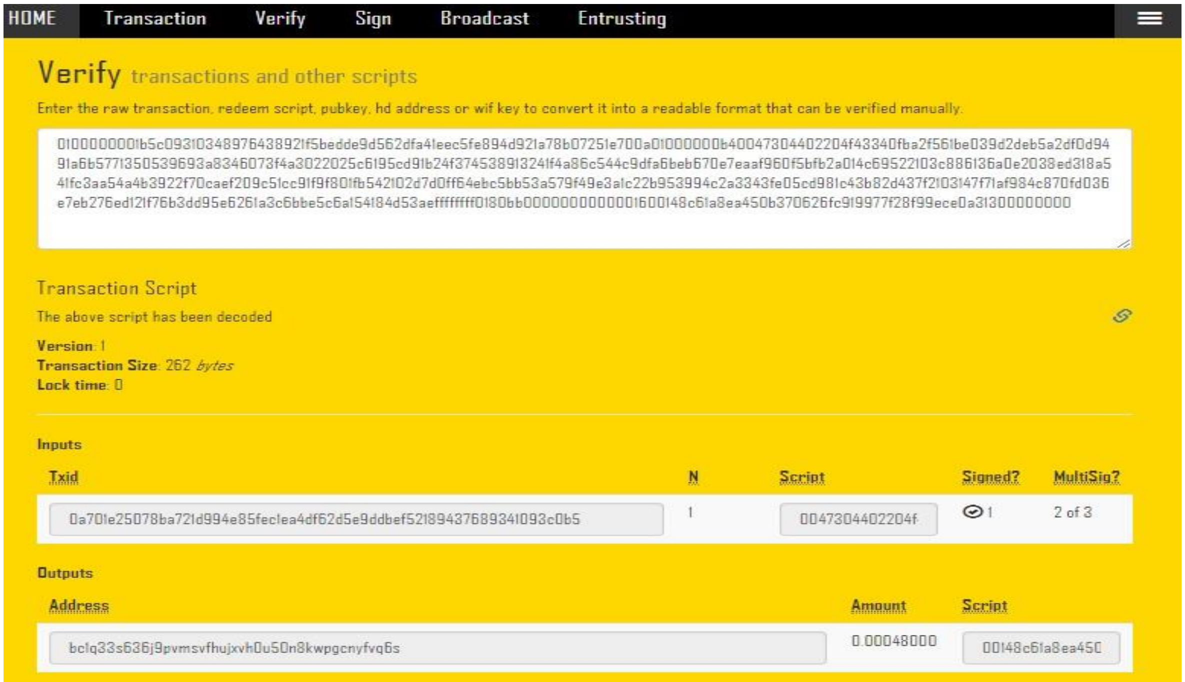
The above transaction has been signed

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000b40047304402204f43340fba2f561be039d2deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9d
fa6beb670e7eaaf960f5bfb2a014c69522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3
dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

Size: 262 *bytes*

This transaction has been signed with one private key.

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000b40047304402204f43340fba2f561be039d2
deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb670e7eaaf960f5bfb2a014c69522
103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd
981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c6
1a8ea450b370626fc919977f28f99ece0a31300000000
```



Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000b40047304402204f43340fba2f561be039d2deb5a2df0d94
91a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb670e7eaaf960f5bfb2a014c69522103c886136a0e2038ed318a5
41fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036
e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

Transaction Script

The above script has been decoded

Version: 1
Transaction Size: 262 *bytes*
Lock time: 0

Inputs

Txid	N	Script	Signed?	MultiSig?
0a701e25078ba721d994e85fec1ea4df62d5e9ddbef52189437689341093c0b5	1	0047304402204f	1	2 of 3

Outputs

Address	Amount	Script
bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s	0.00048000	00148c61a8ea450

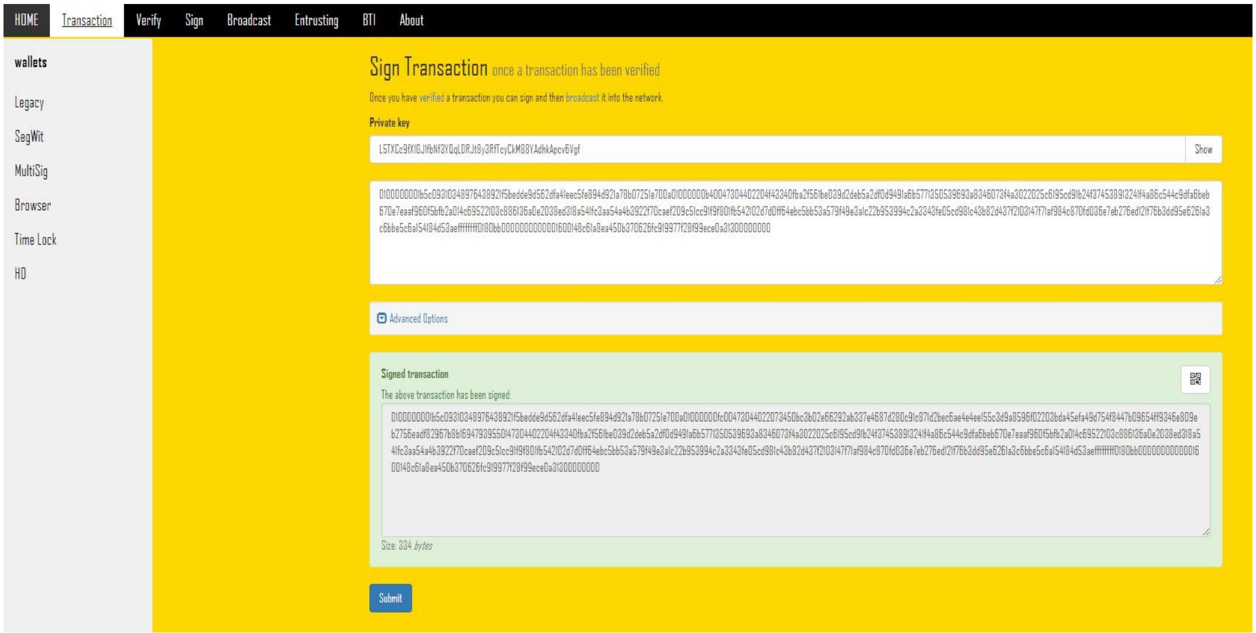
Step 5

Using 3RD PARTY smart contract, delayed text/email message or personal custodian, set up to deliver the raw transaction to Will receiver at a specific future date or circumstance.

The need for the 3RD party here is precisely what you chose, but it comes after the contract being enforced, not before. For that reason, the fund is safe even if the raw transaction held by a 3rd party or become public.

The above Signed raw transaction can't be executed without one of the remaining two privet keys. One held by the receiver and the other held by the sender. In case the receiver gets the raw transaction before the intended time, we can include time lock to the receiver address.

When the will receiver gets the half signed raw transaction, can now Proceed to sign it with his/her privet key and broadcast to receive the digital asset.



Sign Transaction once a transaction has been verified

Once you have verified a transaction you can sign and then broadcast it into the network.

Private key

L5TXCc9fX1GJ1fbNf3YQqLDRJt8y3RfTcyCkM88YAdhkApcv6Vgf

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000b40047304402204f43340fba2f561be039d2deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb
670e7eaaf960f5bfb2a014c69522103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3
c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

Signed transaction

The above transaction has been signed:

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000fc00473044022073450bc3b02e66292ab337e4687d280c91c871d2bec6ae4e4ee155c3d9a8596f02203bda45efa49d754f8447b09654ff9346e809e
b2756eadf82967b8b16947939550147304402204f43340fba2f561be039d2deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb670e7eaaf960f5bfb2a014c69522103c886136a0e2038ed318a5
41fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb00000000000016
00148c61a8ea450b370626fc919977f28f99ece0a31300000000
```

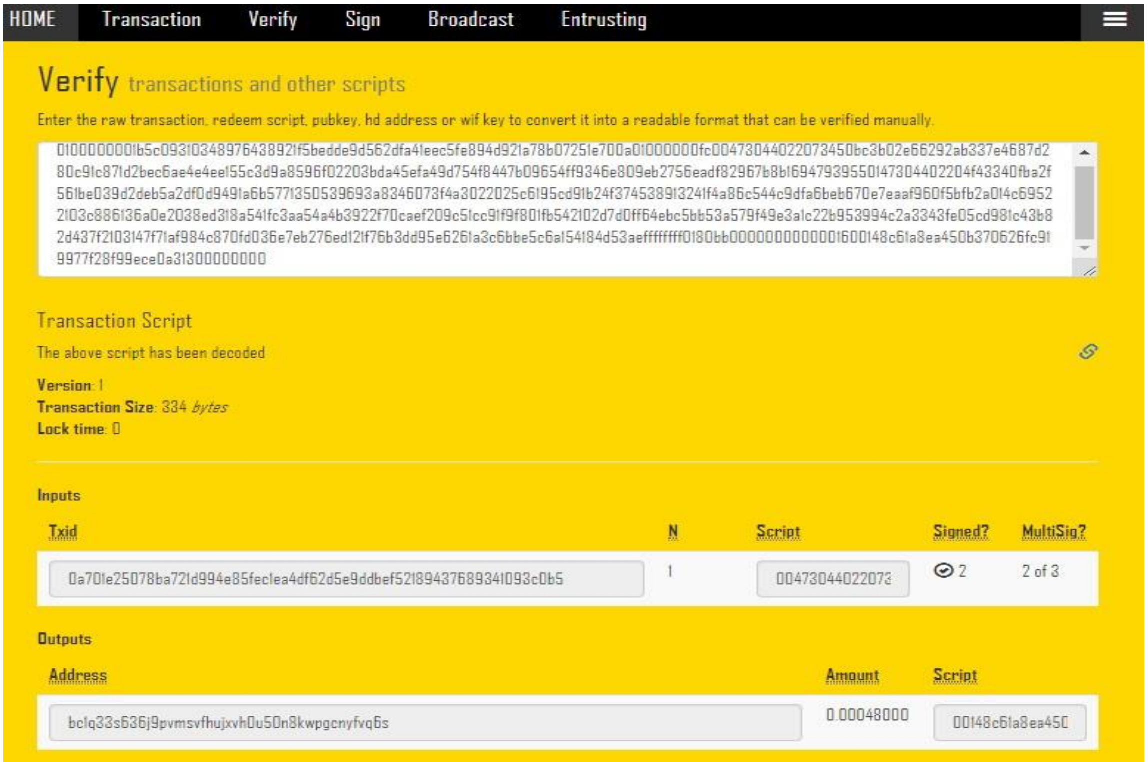
Size: 334 *bytes*

Fully Signed transaction ready to be broadcast

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

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000fc00473044022073450bc3b02e66292ab337e4687d280c9
1c871d2bec6ae4e4ee155c3d9a8596f02203bda45efa49d754f8447b09654ff9346e809eb2756eadf82967b8b16947939550147304402204f43340fba2f561be039
d2deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb670e7eaaf960f5bfb2a014c69522103c886136
a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f
71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc919977f28f99ece0a
31300000000
```

Verify http://will-wallet.com/#verify



Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000fc00473044022073450bc3b02e66292ab337e4687d2
80c91c871d2bec6ae4e4ee155c3d9a8596f02203bda45efa49d754f8447b09654ff9346e809eb2756eadf82967b8b16947939550147304402204f43340fba2f
561be039d2deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb670e7eaaf960f5bfb2a014c6952
2103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b8
2d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b370626fc91
9977f28f99ece0a31300000000
```

Transaction Script

The above script has been decoded

Version: 1
Transaction Size: 334 *bytes*
Lock time: 0

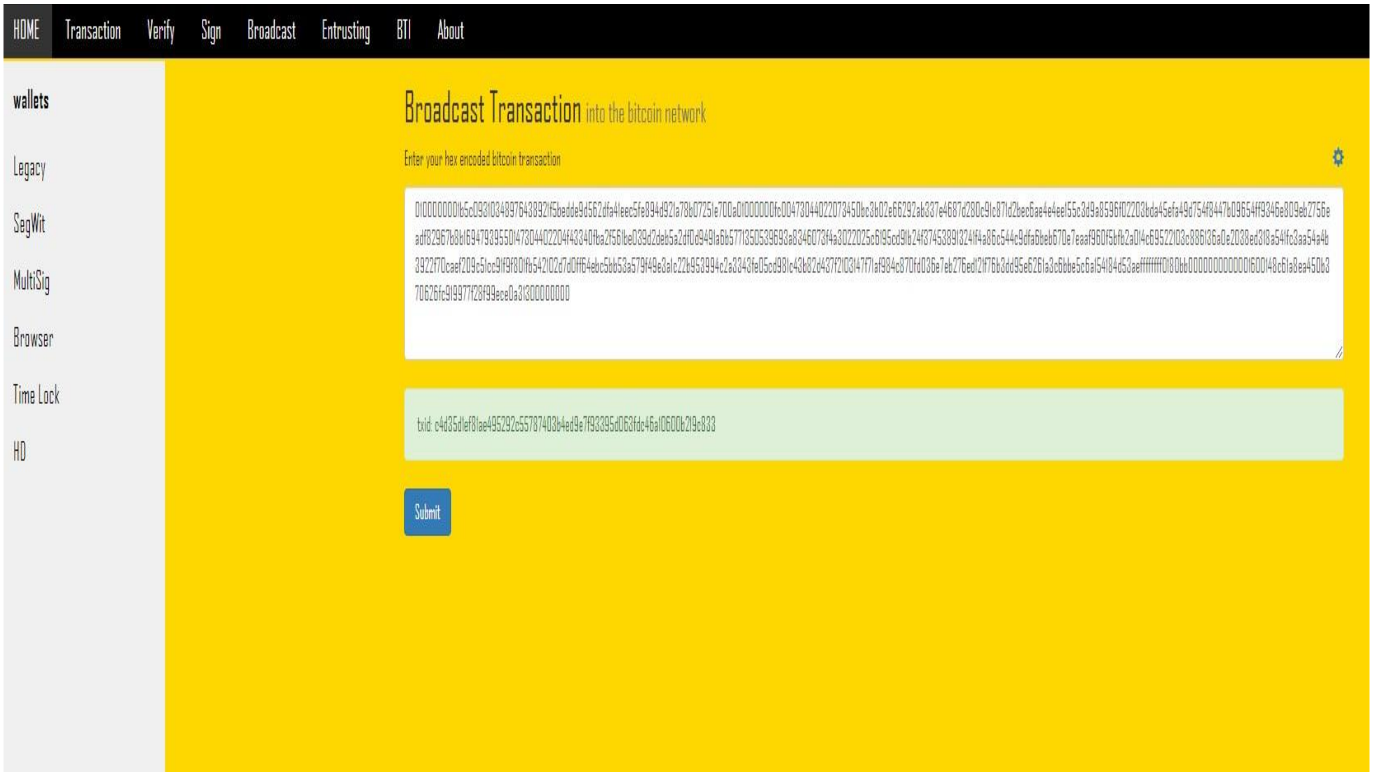
Inputs

Txid	N	Script	Signed?	MultiSig?
0a701e25078ba721d994e85fec1ea4df62d5e9ddbef5218943768934 1093c0b5	1	00473044022073	✓ 2	2 of 3

Outputs

Address	Amount	Script
bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s	0.00048000	00148c61a8ea450

Broadcast http://will-wallet.com/#broadcast



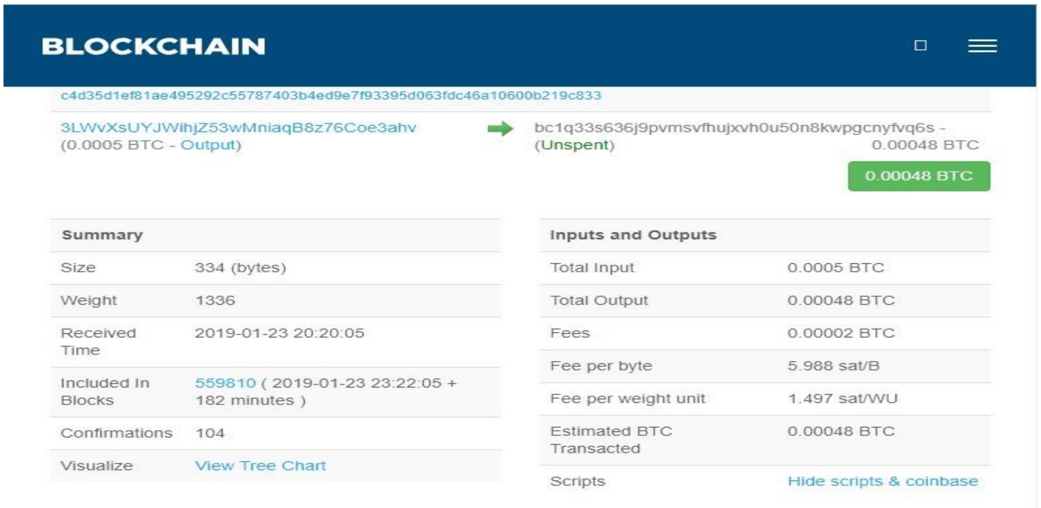
Broadcast Transaction into the bitcoin network

Enter your hex encoded bitcoin transaction

```
0100000001b5c09310348976438921f5bedde9d562dfa41eec5fe894d921a78b07251e700a01000000fc00473044022073450bc3b02e66292ab337e4687d280c91c871d2bec6ae4e4ee155c3d9a8596f02203bda45efa49d754f8447b09654ff9346e809eb2756e
adf82967b8b16947939550147304402204f43340fba2f561be039d2deb5a2df0d9491a6b5771350539693a8346073f4a3022025c6195cd91b24f374538913241f4a86c544c9dfa6beb670e7eaaf960f5bfb2a014c69522103c886136a0e2038ed318a541fc3aa54a4b
3922f70caef209c51cc91f9f801fb542102d7d0ff64ebc5bb53a579f49e3a1c22b953994c2a3343fe05cd981c43b82d437f2103147f71af984c870fd036e7eb276ed121f76b3dd95e6261a3c6bbe5c6a154184d53aeffffffff0180bb0000000000001600148c61a8ea450b3
70626fc919977f28f99ece0a31300000000
```

txid: c4d35d1ef81ae495292c55787403b4ed9e7f93395d063fdc46a10600b219c833

txid: c4d35d1ef81ae495292c55787403b4ed9e7f93395d063fdc46a10600b219c833 https://www.blockchain.com/btc/tx/c4d35d1ef81ae495292c55787403b4ed9e7f93395d063fdc46a10600b219c833



c4d35d1ef81ae495292c55787403b4ed9e7f93395d063fdc46a10600b219c833

3LWvXsUYJWihjZ53wMniaqB8z76Coe3ahv
(0.0005 BTC - Output)

bc1q33s636j9pvmsvfhujxvh0u50n8kwpgcnyfvq6s -
(Unspent) 0.00048 BTC

0.00048 BTC

Summary	
Size	334 (bytes)
Weight	1336
Received Time	2019-01-23 20:20:05
Included In Blocks	559810 (2019-01-23 23:22:05 + 182 minutes)
Confirmations	104
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.0005 BTC
Total Output	0.00048 BTC
Fees	0.00002 BTC
Fee per byte	5.988 sat/B
Fee per weight unit	1.497 sat/WU
Estimated BTC Transacted	0.00048 BTC
Scripts	Hide scripts & coinbase

Now as you can see the fund is in the Will receiver address.

DONE…

Option

To solve early release of fund in the case of receiver get the raw half signed transaction before the intended time or we like to give the raw transaction to the receiver without involving 3rd party to hold until the intended time.

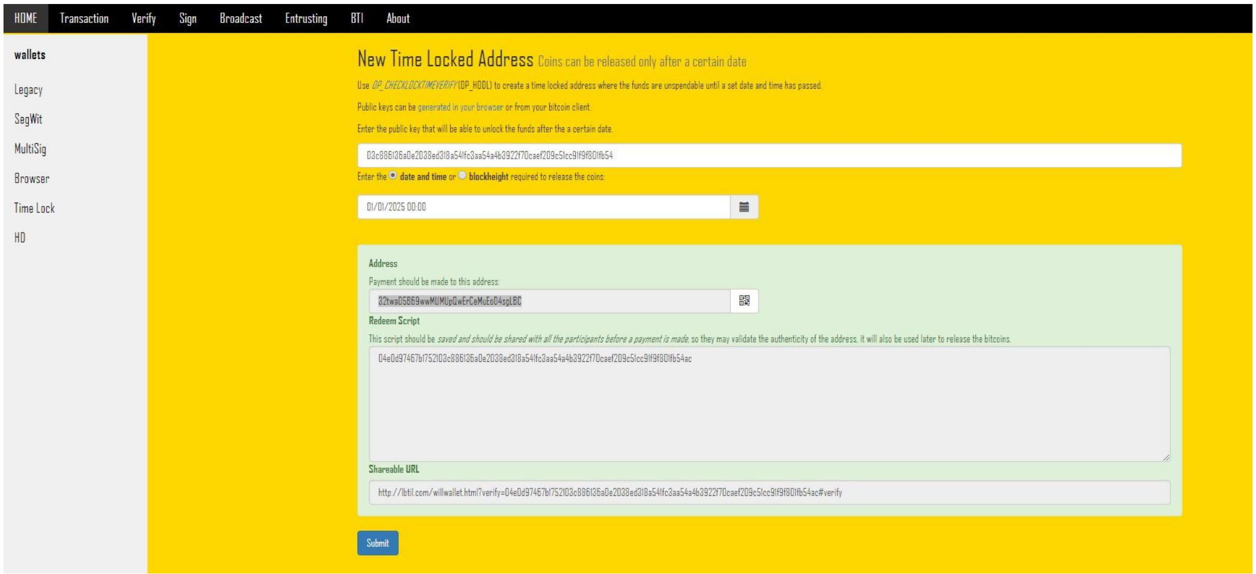
Include Step 2.5

OP_CHECKLOCKTIMEVERIFY: http://will-wallet.com/#newTimeLocked

Create New Time Locked Addresses from the original Public keys of the Will receiver and the fund can be released only after a certain specific date the sender set up.

OP_CHECKLOCKTIMEVERIFY (OP_HODL) to create a time locked address where the funds cannot be spent until a set date and time has passed.

Public key of receiver :03c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54



New Time Locked Address Coins can be released only after a certain date

Use *OP_CHECKLOCKTIMEVERIFY* (OP_HODL) to create a time locked address where the funds are unspendable until a set date and time has passed.

Public keys can be generated in your browser or from your bitcoin client.

Enter the public key that will be able to unlock the funds after the a certain date.

03c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54

Enter the ● **date and time** or ○ **blockheight** required to release the coins:

01/01/2025 00:00

Address

Payment should be made to this address:

32twaD5B69wwMUMUpQwErCeMuEoD4sgLBC

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.

04e0d97467b1752103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54ac

Shareable URL

http://lbtil.com/willwallet.html?verify=04e0d97467b1752103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54ac#verify

Fund release date set by sender 01/01/2025 00:00 transaction should be made to this receiver

address: 32twaD5B69wwMUMUpQwErCeMuEoD4sgLBC

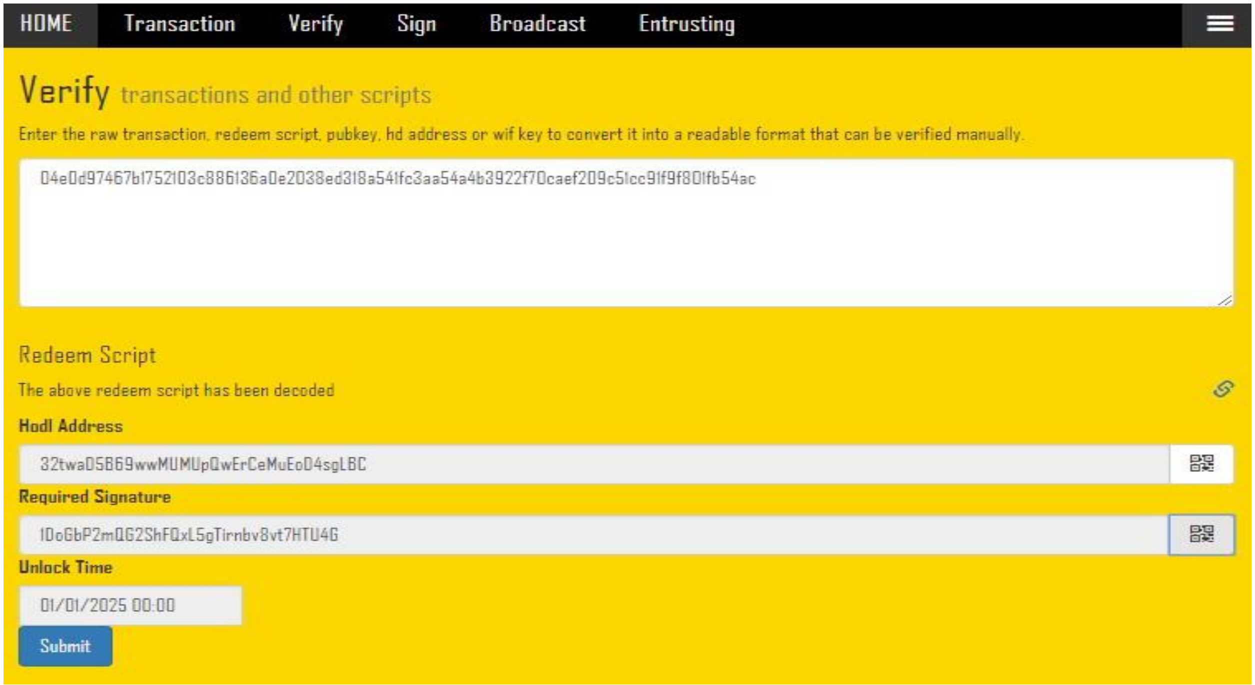
Redeem Script

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.

04e0d97467b1752103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54ac Required

Signature

1DoGbP2mQG2ShFQxL5gTirnbv8vt7HTU4G



Verify transactions and other scripts

Enter the raw transaction, redeem script, pubkey, hd address or wif key to convert it into a readable format that can be verified manually.

04e0d97467b1752103c886136a0e2038ed318a541fc3aa54a4b3922f70caef209c51cc91f9f801fb54ac

Redeem Script

The above redeem script has been decoded

Hodl Address

32twaD5B69wwMUMUpQwErCeMuEoD4sgLBC

Required Signature

1DoGbP2mQG2ShFQxL5gTirnbv8vt7HTU4G

Unlock Time

01/01/2025 00:00

Then repeat the same process from Step 3.

Will wallet:

Provide much more versatility, security and flexibility without 3rd party trust.

1. Digital asset can be released any time before the receiver receives the signed transaction by the sender if necessary.

2. The fund can be used any time before the receiver excite the transaction. If the fund replaced with adequate funding the transaction still be executable upon broadcast.

3. If things change, receiver no longer need it or lost his personal wallet privet key it can be resigned to a different receiving address, with the two pk the sender hold.

4. We can also include more than one wallet address in one transaction for someone want his asset to be divided between several receivers.

5. Only one receiver required to sign the second signature and broadcast the transaction. All receive the fund into their personal wallet simultaneously.

Conclusion

Will wallet solve the problem of transferring inheritance or any found upon unfortunate circumstance like the holder of digital asset passing or any reasons restrict the holder to transfer his/her asset if setup ahead. The possibility of this method is not limited to the above use case, it can be implemented in different custodian solution like estate transferal, monthly payout trust fund, insurance payout and exchanges. It also can be implemented for any digital asset support multi signature wallet.

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

References

[1] “https://github.com/OutCast3k/coinbin/.

[2] Tomoya Ishizaki, " https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki "