Yuhui Dai (yd229)

1

The ERC20 contract address is: 0x8B6565b970b71D945f79BFAEDF51b6962b7FA185

2

The Winning contract address is: 0x292E468240a3524124e2cCb21e4f10EdE9Bec896

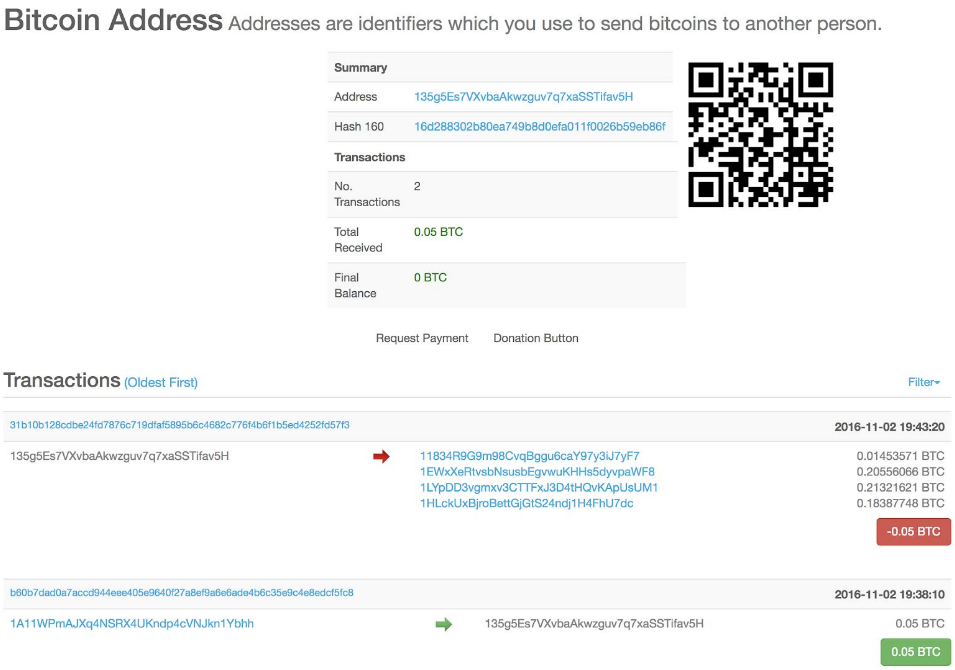
3.1
B4d44f7f598c8ce17292fc883817afc2175a5a40d9e0c58f is Rafael's key

3.2
One potential vulnerability is that the user can produce invalid transactions on the chain via double spending. After 192 transactions, we could only observe < 192 bits, depending how many times such user produces invalid transactions.
To mitigate such issues, the backdoor should only allow user to produce valid transaction on each block so that the chain is intact w.r.t user's secret key.

3.3
The scheme can be modified to leak a user's PK 2 bits at a time, thus reducing the time to reveal the entire secret key to half.

4.
The tumblers have almost the same amount transaction value as the output. The outputs happen after tumbler transactions by a short delay time. The differences in values are due to the transaction fee. As we can see, mixing bitcoin won't completely solve the anonymity issue.The 4 tumbler and output pairs down below:

135g5Es7VXvbaAkwzguv7q7xaSSTifav5H (Bitcoin Fog - foggeddriztrcar2.onion)
Sends to
13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	135g5Es7VXvbaAkwzguv7q7xaSSTifav5H
Hash 160	16d288302b80ea749b8d0efa011f0026b59eb86f
Transactions	
No. Transactions	2
Total Received	0.05 BTC
Final Balance	0 BTC

Transactions (Oldest First)

31b10b128cdbe24fd7876c719dfaf5895b6c4682c776f4b6f1b5ed4252fd57f3 **2016-11-02 19:43:20**

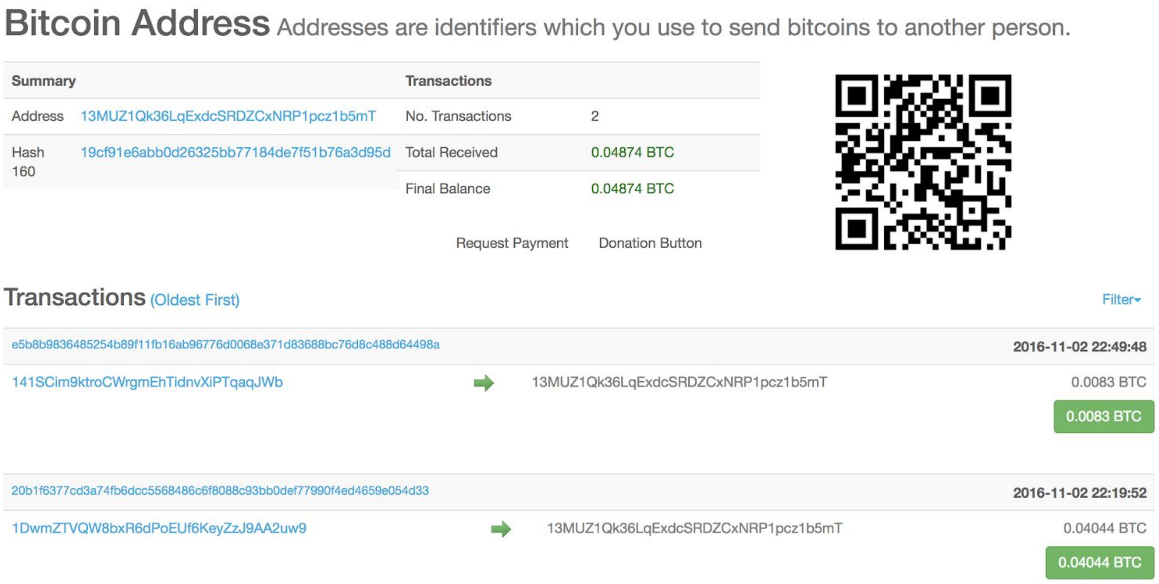
135g5Es7VXvbaAkwzguv7q7xaSSTifav5H → 11834R9G9m98CvqBggu6caY97y3iJ7yF7 0.01453571 BTC
1EWxXeRtvsbNsusbEgvwuKHHs5dyvpaWF8 0.20556066 BTC
1LYpDD3vgmxv3CTTFxJ3D4tHQvKApUsUM1 0.21321621 BTC
1HLckUxBjroBettGjGtS24ndj1H4FhU7dc 0.18387748 BTC

-0.05 BTC

b60b7dad0a7accd944eee405e9640f27a8ef9a6e6ade4b6c35e9c4e8edcf5fc8 **2016-11-02 19:38:10**

1A11WPmAJXq4NSRX4UKndp4cVNJkn1Ybhh → 135g5Es7VXvbaAkwzguv7q7xaSSTifav5H 0.05 BTC

0.05 BTC



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT	No. Transactions	2
Hash 160	19cf91e6abb0d26325bb77184de7f51b76a3d95d	Total Received	0.04874 BTC
		Final Balance	0.04874 BTC

Transactions (Oldest First)

e5b8b9836485254b89f11fb16ab96776d0068e371d83688bc76d8c488d64498a **2016-11-02 22:49:48**

141SCim9ktroCWrgmEhTidnvXiPTqaqJWb → 13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT 0.0083 BTC

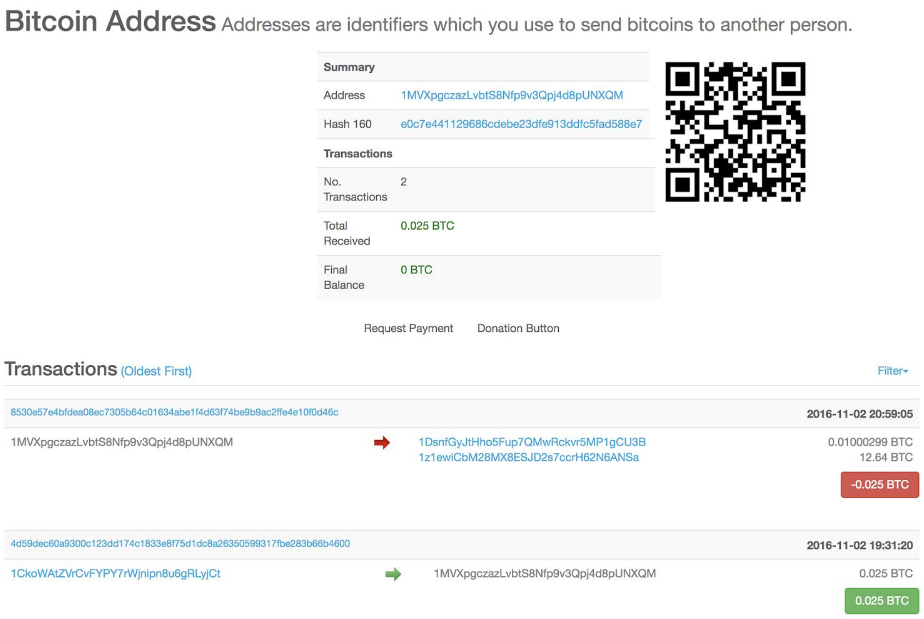
0.0083 BTC

20b1f6377cd3a74fb6dcc5568486c6f8088c93bb0def77990f4ed4659e054d33 **2016-11-02 22:19:52**

1DwmZTVQW8bxR6dPoEUf6KeyZzJ9AA2uw9 → 13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT 0.04044 BTC

0.04044 BTC

1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM (Grams Helix - grams7enufi7jmdl.onion/helix)
Sends to
1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM
Hash 160	e0c7e441129686cdebe23dfe913ddfc5fad588e7
Transactions	
No. Transactions	2
Total Received	0.025 BTC
Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

Filter▾

8530e57e4bfdea08ec7305b64c01634abe1f4d63f74be9b9ac2ffe4e10f0d46c **2016-11-02 20:59:05**

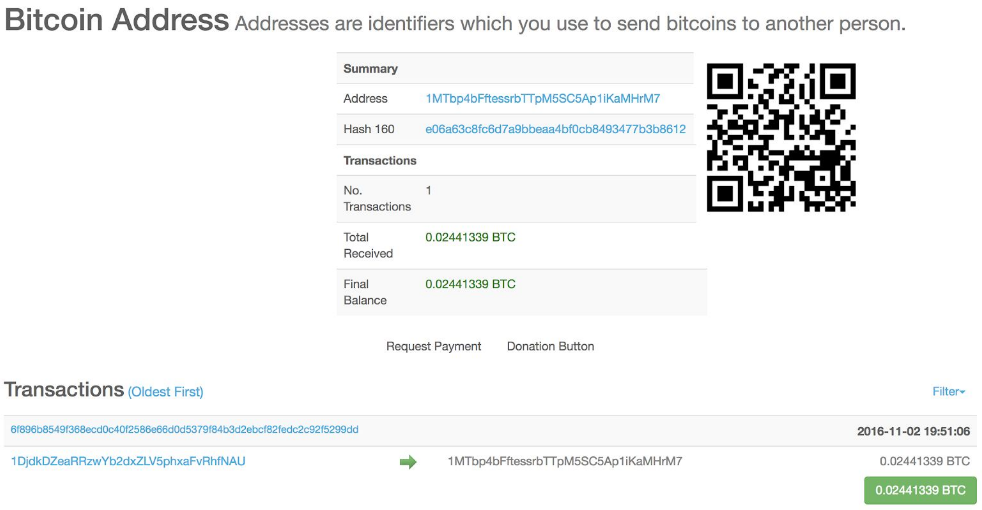
1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM → 1DsnfGyJtHho5Fup7QMwRckvr5MP1gCU3B 0.01000299 BTC
1z1ewiCbM28MX8ESJD2s7ccrH62N6ANSa 12.64 BTC

-0.025 BTC

4d59dec60a9300c123dd174c1833e8f75d1dc8a26350599317fbe283b66b4600 **2016-11-02 19:31:20**

1CkoWAtZVrCvFYPY7rWjnipn8u6gRLyjCt → 1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM 0.025 BTC

0.025 BTC



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7
Hash 160	e06a63c8fc6d7a9bbeaa4bf0cb8493477b3b8612
Transactions	
No. Transactions	1
Total Received	0.02441339 BTC
Final Balance	0.02441339 BTC

Request Payment Donation Button

Transactions (Oldest First)

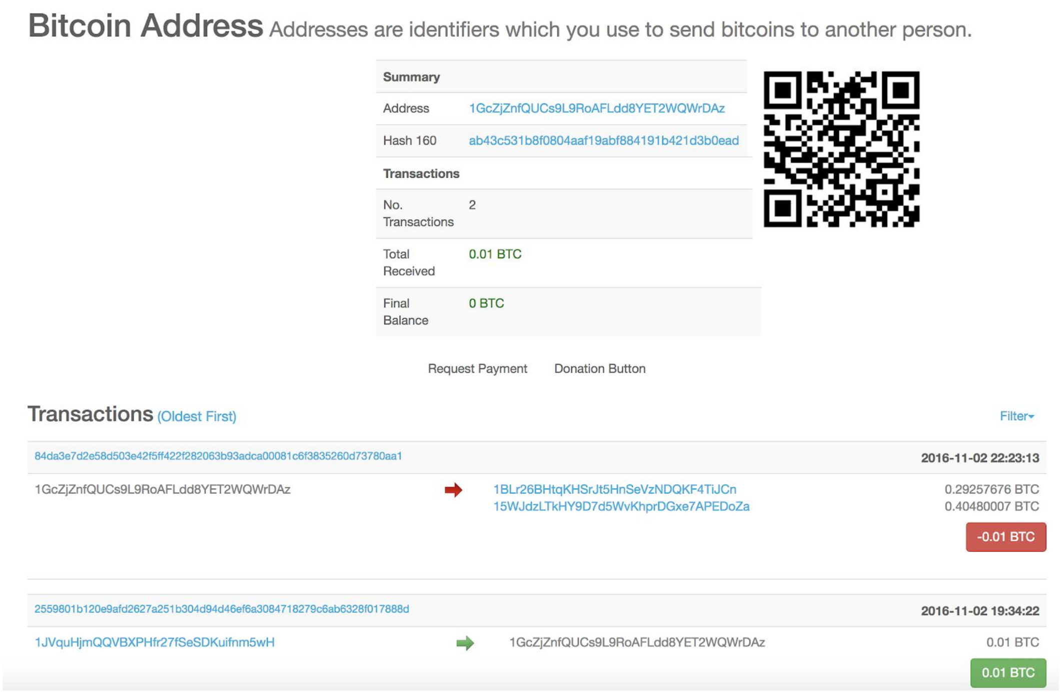
Filter▾

6f896b8549f368ecd0c40f2586e66d0d5379f84b3d2ebcf82fedc2c92f5299dd **2016-11-02 19:51:06**

1DjdkDZeaRRzwYb2dxZLV5phxaFvRhfNAU → 1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7 0.02441339 BTC

0.02441339 BTC

1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz (CoinCloud - coincloud25txgdf.onion)
Sends to
18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz
Hash 160	ab43c531b8f0804aaf19abf884191b421d3b0ead
Transactions	
No. Transactions	2
Total Received	0.01 BTC
Final Balance	0 BTC

Transactions (Oldest First)

84da3e7d2e58d503e42f5ff422f282063b93adca00081c6f3835260d73780aa1 **2016-11-02 22:23:13**

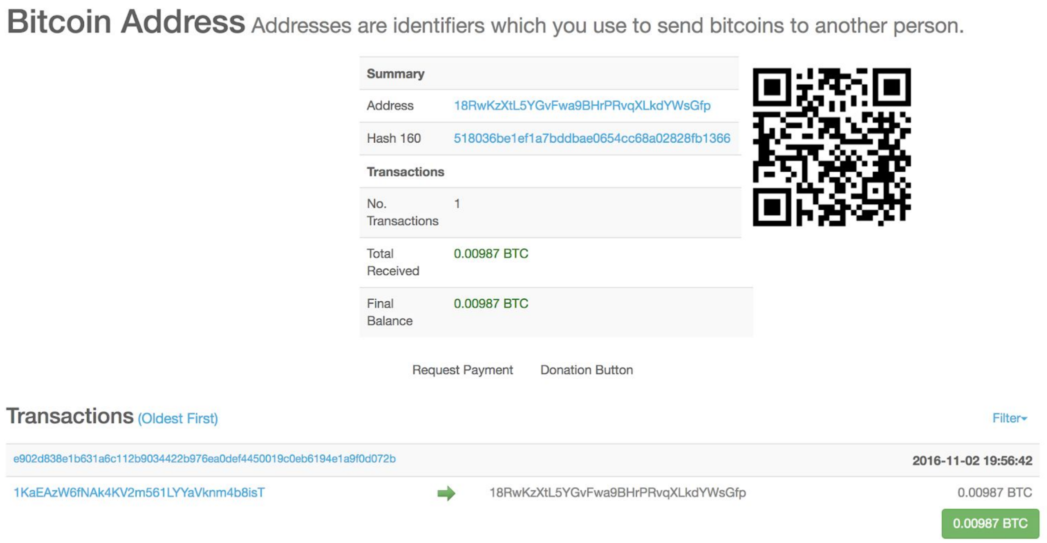
1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz ➡ 1BLr26BHtqKHSrJt5HnSeVzNDQKF4TiJCn 0.29257676 BTC
15WJdzLTkHY9D7d5WvKhprDGxe7APEDoZa 0.40480007 BTC

-0.01 BTC

2559801b120e9afd2627a251b304d94d46ef6a3084718279c6ab6328f017888d **2016-11-02 19:34:22**

1JVquHjmQQVBXPHfr27fSeSDKuifnm5wH ➡ 1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz 0.01 BTC

0.01 BTC



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp
Hash 160	518036be1ef1a7bddbae0654cc68a02828fb1366
Transactions	
No. Transactions	1
Total Received	0.00987 BTC
Final Balance	0.00987 BTC

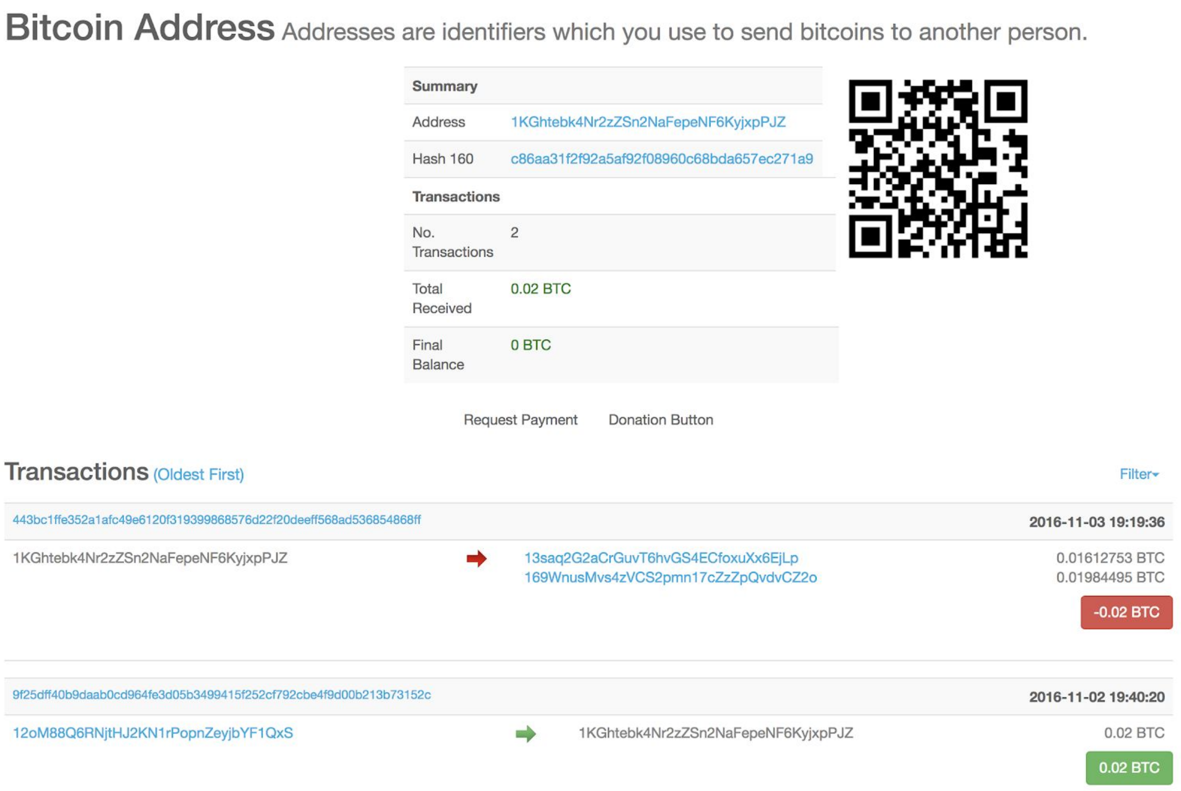
Transactions (Oldest First)

e902d838e1b631a6c112b9034422b976ea0def4450019c0eb6194e1a9f0d072b **2016-11-02 19:56:42**

1KaEAzW6fNAk4KV2m561LYYaVknm4b8isT ➡ 18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp 0.00987 BTC

0.00987 BTC

1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ (PenguinMixer - penguinsmbshtgmf.onion)
Sends to
1BCaztysy2paguXjuC8c652vckNMks69ce



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ
Hash 160	c86aa31f2f92a5af92f08960c68bda657ec271a9
Transactions	
No. Transactions	2
Total Received	0.02 BTC
Final Balance	0 BTC

Transactions (Oldest First)

443bc1ffe352a1afc49e6120f319399868576d22f20deeff568ad536854868ff — **2016-11-03 19:19:36**

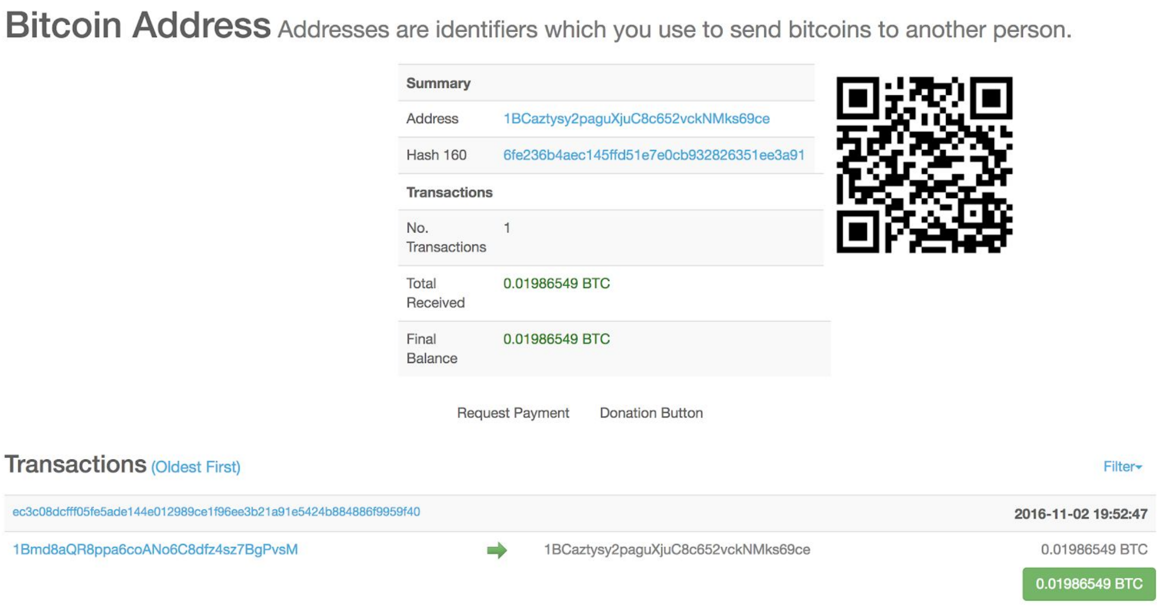
1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ ➡ 13saq2G2aCrGuvT6hvGS4ECfoxuXx6EjLp 0.01612753 BTC
169WnusMvs4zVCS2pmn17cZzZpQvdvCZ2o 0.01984495 BTC

-0.02 BTC

9f25dff40b9daab0cd964fe3d05b3499415f252cf792cbe4f9d00b213b73152c — **2016-11-02 19:40:20**

12oM88Q6RNjtHJ2KN1rPopnZeyjbYF1QxS ➡ 1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ 0.02 BTC

0.02 BTC



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1BCaztysy2paguXjuC8c652vckNMks69ce
Hash 160	6fe236b4aec145ffd51e7e0cb932826351ee3a91
Transactions	
No. Transactions	1
Total Received	0.01986549 BTC
Final Balance	0.01986549 BTC

Transactions (Oldest First)

ec3c08dcfff05fe5ade144e012989ce1f96ee3b21a91e5424b884886f9959f40 — **2016-11-02 19:52:47**

1Bmd8aQR8ppa6coANo6C8dfz4sz7BgPvsM ➡ 1BCaztysy2paguXjuC8c652vckNMks69ce 0.01986549 BTC

0.01986549 BTC

Evaluation:

Appropriate Difficult

Spend 14 hours in total

Appropriate amount of coding