

Deanonymizing Tumbler Users (See Appendix for Screenshots from blockchain)

1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM -> 1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7

Explanation: User with (left) address sent 0.025 BTC and received 0.02441 BTC from Mixer at (right) address

135g5Es7VXvbaAkwzguv7q7xaSSTifav5H -> 13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT

Explanation: User with (left) address sent 0.05 BTC and received 0.0487BTC from Mixer at (right) address

1GcZjZnfQUcs9L9RoAFLdd8YET2WQWrDAz -> 18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp

Explanation: User with (left) address sent 0.01 BTC and received 0.00987 BTC from Mixer at (right) address

1KGhtebk4Nr2zZSn2NaFepNF6KyjxpPJZ -> 1BCaztysy2paguXjuC8c652vckNMks69ce

Explanation: User with (left) address sent 0.02 BTC and received 0.01986 BTC from Mixer at (right) address

Comments: Tumblers and mixers don't always yield privacy. When players send unequal amounts of BTC to the service they need to recover those funds which can also deanonymize the player like in this example. By analyzing how much BTC a user paid the mixer and how much they retrieved, it is not too difficult to associate the input and output addresses associated with the movement of funds. See appendix that shows the color coordinated inputs and output addresses with the transfer of UTXO's.

Appendix

Input: 1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM (Grams Helix - grams7enufi7jmdl.onion/helix)

Fee	0.00270917 BTC (78.232 sat/B - 19.558 sat/WU - 3463 bytes)	-0.02500000 BTC
Hash	8530e57e4bfdea08ec7305b64c01634abe1f4d63f74be9b9ac2ffe4e10f0d...	2016-11-02 17:20
	<div><div>18voLAsdQvuW6PekZaKmpFy2jdboYgjtY0.40705682 BTC</div><div>1DSD5KR2NKuCQmb1wFBubEYaaorCiDwrW30.30552621 BTC</div><div>1MXaztvtwE9xNZG9SZRXW22dNaNadgTX6K0.01000792 BTC</div><div>17z6uSkpiV8vWCy3j6yGFNjdDpmPXijaRL0.20200000 BTC</div><div>1L5xi7KSc8zZEXEtZD2MfVcgaFawKHYN7f0.06316525 BTC</div><div>1AZTpnvV3zy9iegMDFLAj3pQ6NLHwW4Wft3.51000000 BTC</div><div>124KG9nEn7L7RpBXtcCGb554thxzZXm6gG0.13000000 BTC</div><div>1GSH7XrpdUTi8XzEpCXB57P9cHeg4Zeq830.42513061 BTC</div><div>1ScvB4XQn7JeqZAxnt69f669g5RZQocbn0.01000000 BTC</div><div>1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM0.02500000 BTC</div></div> <div>Load more inputs... (13 remaining)</div>	<div><div>1DsrfGyJtHho5Fup7QMwRckvr5MP1gCU3B0.01000299 BTC</div><div>1z1ewiCbM28MX8ESJD2s7ccrH62N6ANSA12.64000000 BTC</div></div>
Fee	0.00011300 BTC (50.222 sat/B - 12.556 sat/WU - 225 bytes)	+0.02500000 BTC
Hash	4d59dec60a9300c123dd174c1833e8f75d1dc8a26350599317fbc283b66...	2016-11-02 15:33
	<div><div>1CkoWATZVrCvFYPy7rWjnpi8u6gRLyJct0.20000000 BTC</div><div>1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM0.02500000 BTC</div><div>1JVquHjmQQVBXPHfr27fSeSDKuifnm5wH0.17488700 BTC</div></div>	

1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7

Transactions

Fee	0.00018278 BTC (62.382 sat/B - 15.596 sat/WU - 293 bytes)	+0.02441339 BTC
Hash	6f896b8549f368ecd0c40f2586e66d0d5379f84b3d2ebcf82fedc2c92f52...	2016-11-02 15:52
	<div><div>1DjdkDZeaRRzwYb2dxZLV5phxaFvRhNAU10.82352037 BTC</div><div>15yncsJ7RsneaDnSmN1UgJ98rjZY3kJGmY0.09869140 BTC</div><div>1JJPCjkdqDJTzQpPAkaHWFoy3CWcEpVYVE10.66415780 BTC</div><div>16NrteLwftBLAm8mXw11rfcd1bwxMvF0.03667500 BTC</div><div>1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM70.02441339 BTC</div></div>	

Nikhil Pereira
CS5433 – HW3 Solutions.pdf
Question 3: What Anonymity?
April 12, 2022

Input: 135g5Es7VXvbaAkwzguv7q7xaSSTifav5H (Bitcoin Fog - foggeddriztrcar2.onion)

Transactions ⓘ

Fee	0.00010310 BTC (10.000 sat/B - 2.500 sat/WU - 1031 bytes)	-0.05000000 BTC
Hash	31b10b128cbe24fd7876c719dfa5895b6c4682c776f4b6f1b5ed4252fd5...	2016-11-02 15:49
	<div>135g5Es7VXvbaAkwzguv7q7xaSSTifav5H 0.05000000 BTC →</div> <div>1Aq3fN6Yk8wn53yXv1UkL1mrsQEcpRWz 0.05000000 BTC</div> <div>1Fq21MjXYtXQscrFEVBvwwABiKRK3bHE8 0.12283818 BTC</div> <div>1BufZKAifKY4xdLK6c8mTsmCkUewGppPSS 0.04640052 BTC</div> <div>1726b7DqxzhqAkYoiQw9n5zTDoEZkbTVt1 0.33700000 BTC</div> <div>16isi6sz7hWTs8UoZQBqmU99meUmA7FxBD 0.01105446 BTC</div> <div>11834R9G9m98CvqBggv6caY97y3iJ7yF7 0.01453571 BTC</div> <div>1EWxXeRtvsbNsubEgwwuKHHs5dyvpaWF8 0.20556066 BTC</div> <div>1LYpDD3vgmxv3CTTFxJ3D4tHQvKApUsUM1 0.21321621 BTC</div> <div>1HLckUxBjroBettGjGtS24ndj1H4FhU7dc 0.18387748 BTC</div>	
Fee	0.00011300 BTC (50.222 sat/B - 12.556 sat/WU - 225 bytes)	+0.05000000 BTC
Hash	b60b7dad0a7acc944eee405e9640f27a8ef9a6e6ade4b6c35e9c4e8edc...	2016-11-02 15:42
	<div>1A11WPmAJXq4NSRX4UKndp4cVNJkn1Ybhh 0.16477400 BTC →</div> <div>135g5Es7VXvbaAkwzguv7q7xaSSTifav5H 0.05000000 BTC</div> <div>12oM88Q6RNjtHJ2KN1rPopnZeyjbYF1QxS 0.11466100 BTC</div>	

13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT

Transactions ⓘ

Fee	0.00002260 BTC (10.044 sat/B - 2.511 sat/WU - 225 bytes)	+0.04044000 BTC
Hash	20b1f6377cd3a74fb6dcc5568486c6f8088c93bb0def77990f4ed4659e05...	2016-11-02 21:08
	<div>1DwmZTVQW8bxR6dPoEUf6KeyZzJ9AA2uw9 0.10355413 BTC →</div> <div>1JdwbKtmsnguwNGMPhoiZF58UVmEpNpG 0.06309153 BTC</div> <div>13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT 0.04044000 BTC</div>	
Fee	0.00002260 BTC (10.044 sat/B - 2.511 sat/WU - 225 bytes)	+0.00830000 BTC
Hash	e5b8b9836485254b89f11fb16ab96776d0068e371d83688bc76d8c488d...	2016-11-02 21:08
	<div>141SCim9ktroCWrgmEhTidnvXIPTqaqJWb 0.10461307 BTC →</div> <div>13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT 0.00830000 BTC</div> <div>1KxWRzfsUBKQbPh58a6wCKNfgQdKjcWmtb 0.09629047 BTC</div>	

Nikhil Pereira
CS5433 – HW3 Solutions.pdf
Question 3: What Anonymity?
April 12, 2022

Input: 1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz (CoinCloud - coincloud25txgdf.onion)

Transactions ⓘ

Fee	0.00042832 BTC (52.619 sat/B - 13.155 sat/WU - 814 bytes)	-0.01000000 BTC
Hash	84da3e7d2e58d503e42f5ff422f282063b93adca00081c6f3835260d737...	2016-11-02 19:13
	<div>1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz 0.01000000 BTC ➡</div> <div>1Ffo58MP7rW3qNczef24hfhXDBSxtznEgf 0.10338573 BTC</div> <div>1DDbf4nfvjhV842rCCapWttPwfN53BaczF 0.12884885 BTC</div> <div>1AJmVhWLXxVTwBaBfGJwbzQm1HhMP4RSVP 0.15591135 BTC</div> <div>1JSF8PktAqbXawmbmsWJmEeCrFnBzBaQk 0.29965922 BTC</div>	<div>1BLr26BhtqKHSrJt5HnSeVzNDQKF4TiJCn 0.29257676 BTC</div> <div>15WJdzLTkHY9D7d5WvKhprDGxe7APEDoZa 0.40480007 BTC</div>
Fee	0.00011300 BTC (50.222 sat/B - 12.556 sat/WU - 225 bytes)	+0.01000000 BTC
Hash	2559801b120e9afd2627a251b304d94d46ef6a3084718279c6ab6328f01...	2016-11-02 15:42
	<div>1JVquHjmQQVBXPHfr27fSeSDKuifnm5wH 0.17488700 BTC ➡</div>	<div>1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz 0.01000000 BTC</div> <div>1A11WPmAJXq4NSRX4UKndp4cVNJkn1Ybhh 0.16477400 BTC</div>

18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp

Transactions ⓘ

Fee	0.00009747 BTC (43.128 sat/B - 10.782 sat/WU - 226 bytes)	+0.00987000 BTC
Hash	e902d838e1b631a6c112b9034422b976ea0def4450019c0eb6194e1a9f0...	2016-11-02 16:02
	<div>1KaEAzW6fNAk4KV2m561LYaVknm4b8isT 0.11335320 BTC ➡</div>	<div>18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp 0.00987000 BTC</div> <div>1Ffo58MP7rW3qNczef24hfhXDBSxtznEgf 0.10338573 BTC</div>

Nikhil Pereira
CS5433 – HW3 Solutions.pdf
Question 3: What Anonymity?
April 12, 2022

Input: 1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ (PenguinMixer - penguinsmbshtgmf.onion)

Transactions ①

Fee	0.00023516 BTC (63.046 sat/B - 15.761 sat/WU - 373 bytes)	-0.02000000 BTC
Hash	443bc1ffe352a1afc49e6120f319399868576d22f20deeff568ad53685486...	2016-11-03 15:30
	1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ 0.02000000 BTC → 19dsqknEQ19hGyJFeFuS7LQCWadMSU3XA 0.01620764 BTC →	13saq2G2aCrGuvT6hvGS4ECfoxuXx6EjLp 0.01612753 BTC 169WnusMvs4zVCS2pmn17cZzZpQvdvCZ2o 0.01984495 BTC
Fee	0.00011300 BTC (50.000 sat/B - 12.500 sat/WU - 226 bytes)	+0.02000000 BTC
Hash	9f25dff40b9daab0cd964fe3d05b3499415f252cf792cbe4f9d00b213b73...	2016-11-02 15:42
	12oM88Q6RNjHJ2KN1rPopnZeyjbYF1QxS 0.11466100 BTC →	1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ 0.02000000 BTC 1EGDuWmxgAWY6fmTZqw5UP3KgD1gnytvmg 0.09454800 BTC

1BCaztysy2paguXjuC8c652vckNMks69ce

Transactions ①

Fee	0.00014221 BTC (63.204 sat/B - 15.801 sat/WU - 225 bytes)	+0.01986549 BTC
Hash	ec3c08dcff05fe5ade144e012989ce1f96ee3b21a91e5424b884886f9959...	2016-11-02 15:53
	1Bmd8aQR8ppa6coAno6C8dfz4sz7BgPvsM 0.03621534 BTC →	19dsqknEQ19hGyJFeFuS7LQCWadMSU3XA 0.01620764 BTC 1BCaztysy2paguXjuC8c652vckNMks69ce 0.01986549 BTC

Evaluation:

- Did you find the homework easy, appropriately difficult, or too difficult? Difficult because solidity is hard to learn and test with windows. Instructions on testing our etheremonlite monster was not clear and led to wasted time and effort.
- How many hours total (excluding breaks :)) were spent on the completion of this assignment? Roughly 12 hours
- Did you feel there was too much coding, the appropriate amount of coding, or not enough coding. There was enough coding just to get out feet wet with smart contracts.