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

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

1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ -> 1BCaztysy2paguXjuC8c652vckNMks69ce

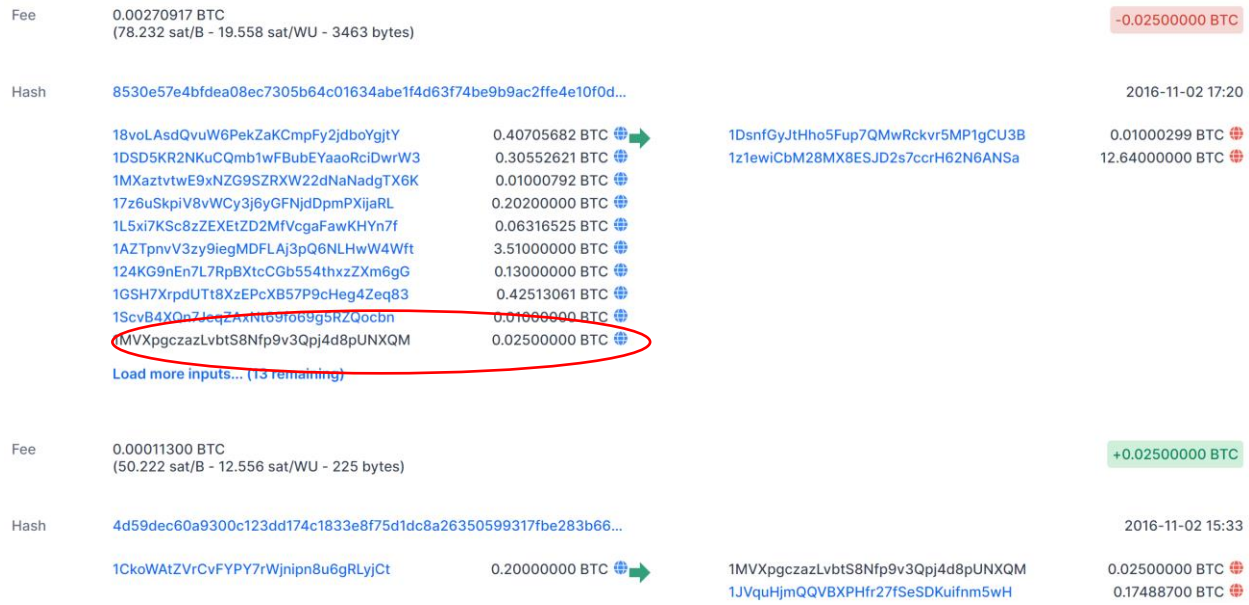
Explanation: User with (left) address sent 0.02 BTC and received 0.01986 BTC from Mixer at (right) address

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.

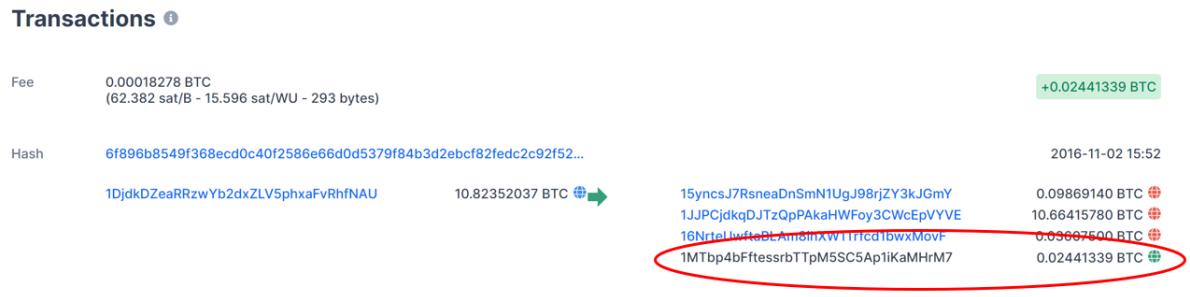
Nikhil Pereira
CS5433 – HW3 Solutions.pdf
Question 3: What Anonymity?
April 12, 2022

Appendix

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



1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7



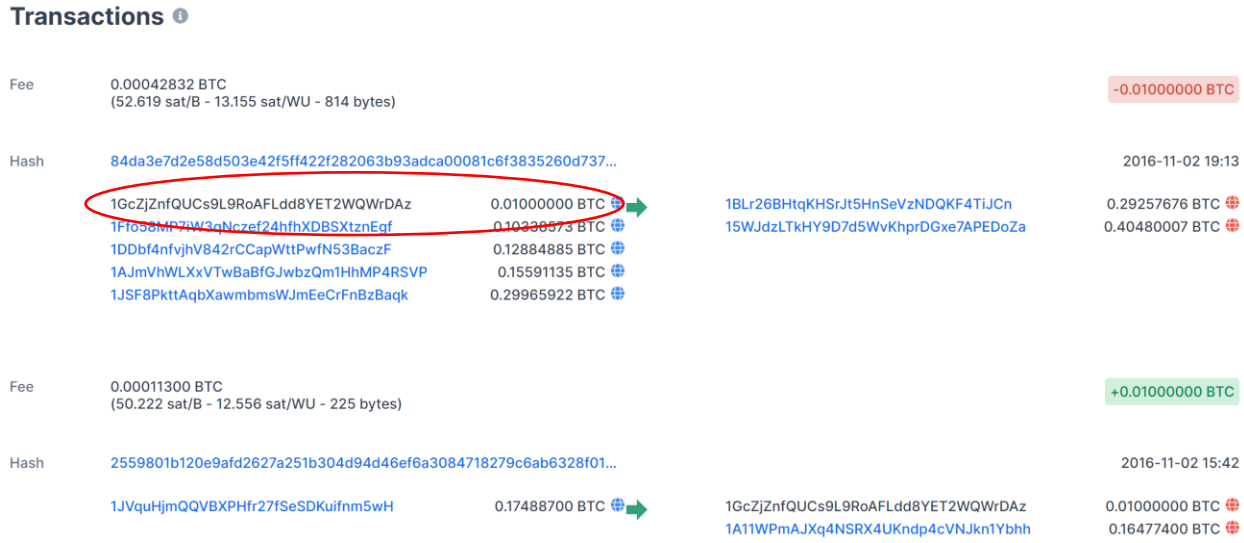
Nikhil Pereira
CS5433 – HW3 Solutions.pdf
Question 3: What Anonymity?
April 12, 2022

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

13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT

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

Input: 1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz (CoinCloud - coincloud25txgdf.onion)

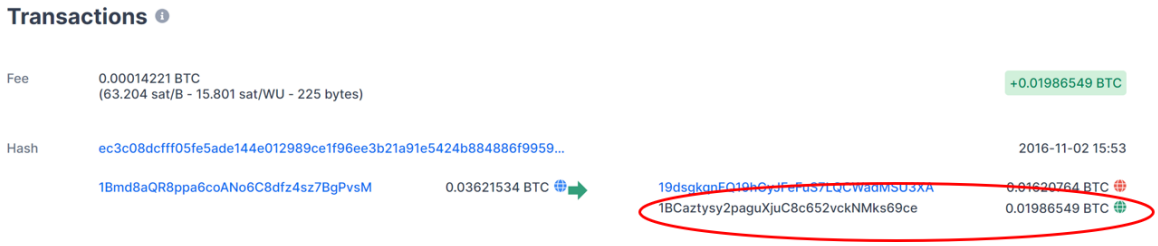


18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp

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

Input: 1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ (PenguinMixer - penguinsmbshtgmf.onion)

1BCaztysy2paguXjuC8c652vckNMks69ce



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.