P2PMIXNOTE

lu562

June 2017

1.dinning cryptographers networks:https://en.wikipedia.org/wiki/Dining_cryptographers_problem

2.DiceMix requires 4+2f rounds in the presence of f malicious peers.

3.bulletin board: a server receiving messsages from each peer and broadcasting them to all other peers.(honest)

4.DiceMix built on synchronous settings. We can replace bulletin board using a reliable broadcast protocol.

5.the input messages must be fresh.(what if all honest nodes want to send messages at the same time, in this scenario all messages are not random)

6.termination is impossible to achieve against a malicious bulletin board, which can just block all communicaation.

7.3 needss: 1.key exchange mechanisms 2. all nodes publish a message simutaneously,3 encuring termination.

8.handling collisions:redundancy.building slots: $S_j = \sum m_i^j$

9.non-malleable commitment. preventing malicious peers from choosing their DC-net vectors depending on DC-net vectors of others. If bulletin board can be trusted then when can omit this.

10.KE-¿CM-¿DC-¿CF if everything OK.

6/12

11.coin mixing. Coinshuffle++. property correct balance.

12.GEN(): create a fresh pair of signing-verification keys and return the verification key to inplement GEN();

13.CONFIRM(): Coinjoin.

14.The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

15.coinjoin:CoinJoin is an anonymization method for bitcoin transactions proposed by Gregory Maxwell. The following idea is behind CoinJoin: When you want to make a payment, find someone else who also wants to make a

payment and make a joint payment together. In case of such a joint payment there will be no way to relate input and outputs in one bitcoin transaction and thus the exact direction of money movement will remain unknown to the third party.

16. CoinShuffe is described as a completely decentralized coin mixing protocol inspired by CoinJoin to ensure security against theft and by the accountable anonymous group communication protocol Dissent to ensure anonymity as well as robustness against DoS attacks.

useful materials:1.https://en.wikipedia.org/wiki/CoinJoin

2.https://bitcoinmagazine.com/articles/shuffling-coins-to-protect-privacy-and-fungibility-a-new-take-on-traditional-mixing-1465934826/

3.https://bitcointalk.org/index.php?topic=567625.0