区块链作业七

SA20225085 朱志儒

1. What is the Birthday Attack?

A birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties. The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations (pigeonholes).

1. What is the ECDSA signatures and how it is used in blockchain?

ECDSA means Elliptic Curve Digital Signature Algorithm, which is defined by an elliptic curve, a generator point of the elliptic curve with large prime order, a large, prime integer and a cryptographic hash function. It is used to ensure that funds can only be spent by their rightful owners in blockchain.

1. What is the difference between Centralized Mixers and Decentralized Mixing Protocol?

In Centralized Mixers, you send coins to third-party mixer address, mixer sends unlinked coins to you sometime in near future to minimize timing information leak. There are counterparty risk, logging risk and centralization risk in Centralized Mixers.

Decentralized Mixing Protocol removes counterparty risk and avoid fees by taking out the middleman. It create a network of peers outside of Bitcoin network who cooperate to make transactions which mix their coins, without relying on a trusted third party.

1. What’s the idea of Anonymity through Mixing on blockchains?

There are many types of Mixing, such as Centralized Mixers, Altcoin Exchange Mixing, Decentralized Mixing Protocols and Privacy-focused Altcoins.

The idea of Centralized Mixers: send coins to third-party mixer address, mixer sends unlinked coins to you sometime in near future to minimize timing information leak；

The idea of Altcoin Exchange Mixing: send dirty funds through several layers of altcoin ⇐⇒ altcoin exchanges to obfuscate money trail;

The idea of Decentralized Mixing Protocols: remove counterparty risk and avoid fees by taking out the middleman;

The idea of CoinSwap: natural extension of centralized mixer: “A mixer that can’t run with your coins.”;

The idea of TumbleBit: improve on CoinSwap so the mixer can’t steal funds and never learns who receives the clean funds;

The idea of CoinJoin: mix together coins in a single n-of-n multisignature transaction;

The idea of JoinMarket: create market of liquidity providers who are willing to mix their coins for a fee;

The idea of CoinParty: decentralized mixing protocol but with better deniability. Want transactions to look the same as normal Bitcoin transactions to passive observers;

The idea of Monero: hide input/output mappings with Ring Signatures. Choose some set of previous outputs to “mix” with. These are then bound with your outputs in a cryptographic ring signature;

The idea of ZCASH: altcoin where transactions reveal nothing about input/output addresses AND input/output values.

1. What’s your experience with Blockchain-Car-Auction\_part1-3?

In part1, I deployed a new business network successfully. In the network, I added three participants. In part2, I added participants and transferred assets in the blockchain. In part3, I explored the editor views and archived data in my business network.