The 35th ACM/SIGAPP Symposium On Applied Computing

PrivateEx: Privacy Preserving Exchange of Crypto-assets on Blockchain

Lei Xu, Lin Chen, Zhimin Gao, Keshav Kasichainula, Miguel Fernandez, Bogdan Carbunar, Weidong Shi

The University of Texas Rio Grande Valley

Agenda

BACKGROUND AND MOTIVATION

CHALLENGES AND PROBLEM STATEMENT

DESIGN OF PRIVATEEX

DISCUSSIONS AND FUTURE WORK

Background and Motivation: Blockchain and cryptocurrency

Bitcoin is the first cryptocurrency that is widely accepted

Bitcoin utilizes the blockchain to get rid of dependency on a third party

Blockchain is a data structure maintained by multiple participants

The concept of cryptocurrency is then extended to crypto asset

In theory anything can be converted to crypto asset and then the ownership can be changed in the cyber world

Background and Motivation: Privacy concerns

The original idea of blockchain construction:

- Disclosing everything to everyone of the system
- The majority of participants are honest

This design philosophy causes privacy concerns

Bitcoin does not provide anonymity protection

A variety of techniques have been proposed to address the privacy concern of blockchain based cryptocurrency

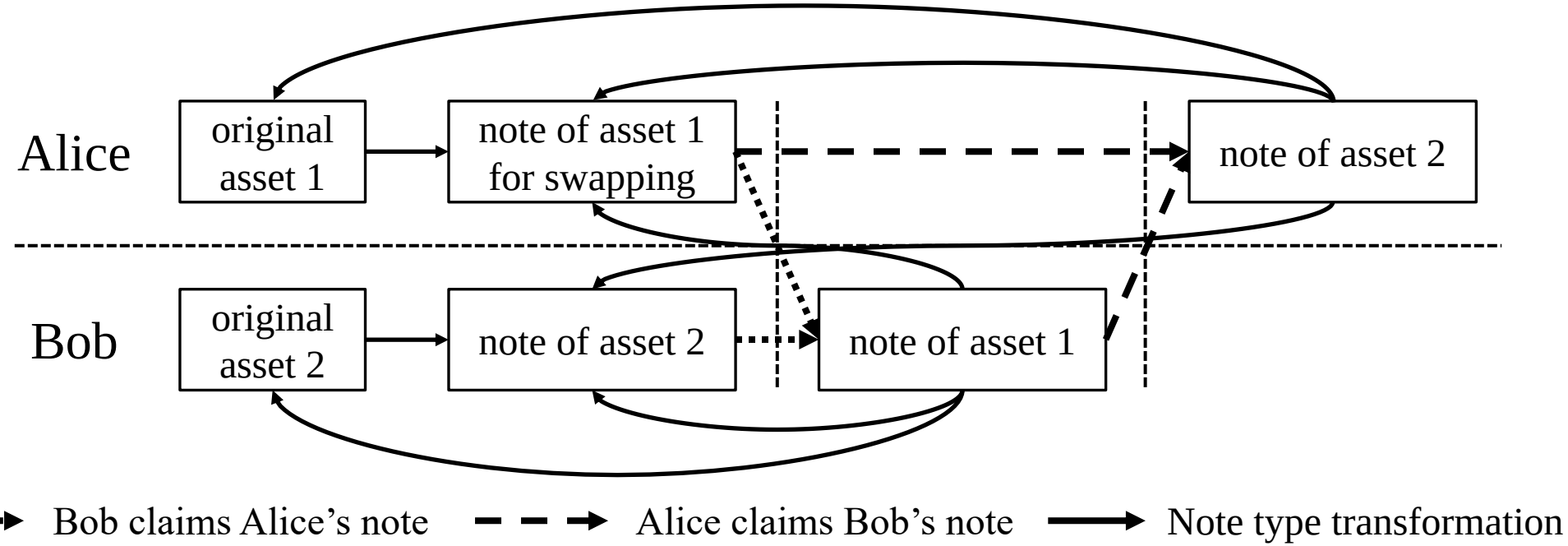
- Mix-net
- Hiding within a group
- Privacy preserving statement verification

Challenges and Problem Statement Exchanging of different assets

- Most of existing works focus on improving the privacy of transactions of a single type of crypto asset
- The problem becomes more interesting when we have more than types of crypto assets
  - Besides one-way transferring, the system needs to support exchange
  - Two users with different types and amounts of crypto assets can exchange their own assets
- Current approaches of supporting crypto assets exchange
  - Centralized exchange platform
  - Blockchain using smart contract
- How can we design a blockchain based privacy preserving exchange platform?

Design of PrivateEx
The overall idea

- Assume Alice and Bob want to exchange their assets



Design of PrivateEx
Key requirements of PrivateEx

- Correctness
  - The user can only exchange using his/her own asset
  - The user cannot create new asset from scratch
  - The user cannot alter the promised asset in the exchange
- Fairness
  - If the exchange succeeds, both parties get the other's asset
  - If the exchange fails, both parties get their assets back
  - There is no third possibility
- Privacy
  - One can only learn information of exchanges that he/she is involved

Design of PrivateEx Correctness

- The correctness feature is guaranteed by the blockchain
  - A unique tag is attached to a note
  - The blockchain only allows the creation of new note from an old one
  - This is similar to the way how Bitcoin prevents double-spending

Design of PrivateEx Fairness

- PrivateEx exchange protocol leverages the blockchain to guarantee fairness
  - Alice creates a new note for exchange which has embedded information of the asset she wants to get
  - If Bob also has a new note for exchange that matches with Alice's demand, they can conduct the exchange
- Either Alice or Bob can initialize the exchange, and the initialization will :
  - Destroy his/her own note
  - Enable the demand part of the other party's note
  - Create a new note for the desired asset
- One can always change his/her mind before the initialization, which will
  - Stop further exchange initialization operation
  - Destropy his/her own note for exchange
  - Create a new note for his/her own

Design of PrivateEx Privacy

- PrivateEx utilizes the ZK-SNARK to hide contents of transactions while allowing everyone to verify their correctness
- The most challenge part is to allow Alice and Bob to finish the exchange in a sequential and non-revocable manner
  - Two tags are embedded in a note for exchange
  - One tag is used for the counter party to continue the exchange, and one tag is used to finish the exchange
  - Proof of knowing a tag without disclosing it is done in a similar way like Zcash with ZK-SNARK
- ZK-SNARK is also used to verify other features
  - The two exchanged notes are compatible,

Potential Future Researches

- Porting crypto assets to different blockchains
- More efficient zero-knowledge proof system for exchange
- Supporting multiparty exchange

STAY ENGAGED.
STAY SAFE.

Questions can be sent to xuleimath@gmail.com