

# Pisces: Private and Compliant Cryptocurrency Exchange

Ya-nan Li, **Tian Qiu**, Qiang Tang

tian.qiu@sydney.edu.au



THE UNIVERSITY OF  
SYDNEY

<https://eprint.iacr.org/2023/1317/>

<https://github.com/yananli117/Pisces>

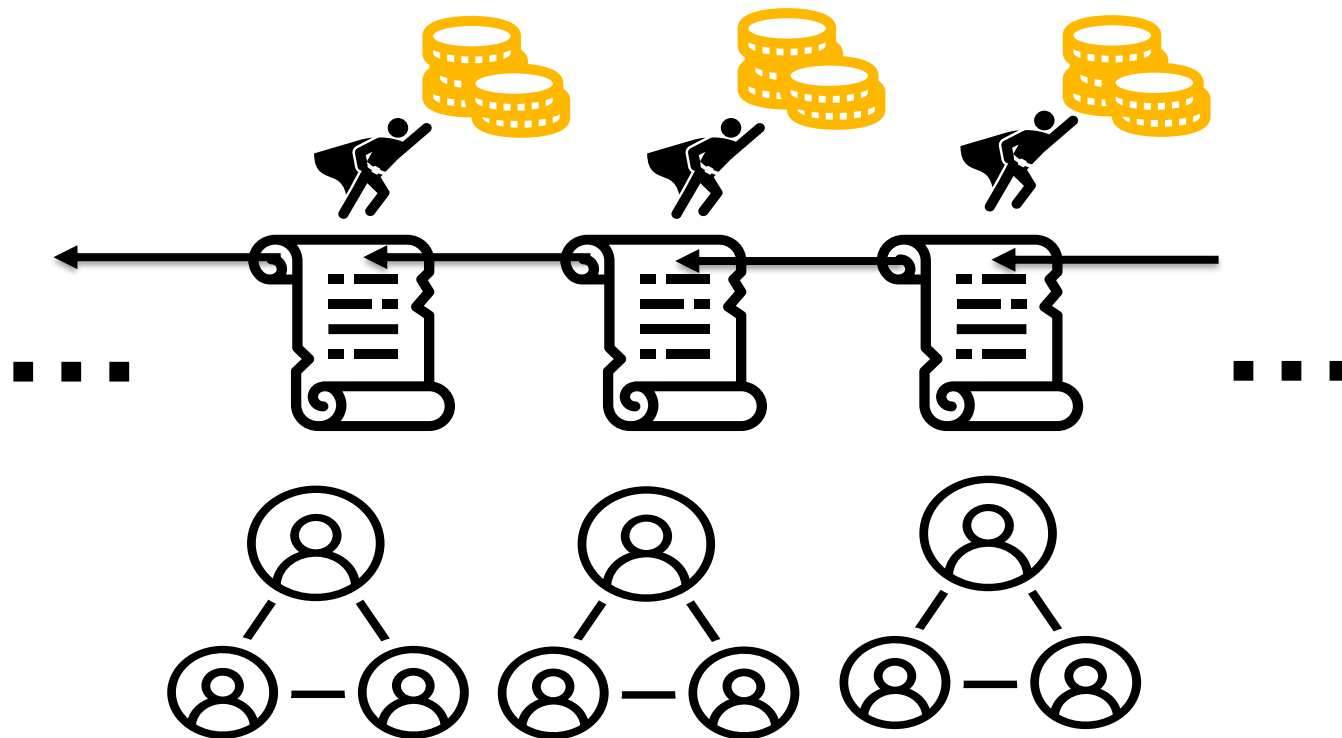


# Overview

- Background
- Privacy issue
- Our goals
- Main challenges
- Our constructions
- Our results
- Open problem
- Take away

# Background

- Blockchain: a publicly distributed ledger
- Cryptocurrency: reward for blockchain miners: Bitcoin, Ether...



# Background

## Centralized exchange platform

– Binance



– Coinbase



# Background

## Centralized exchange platforms

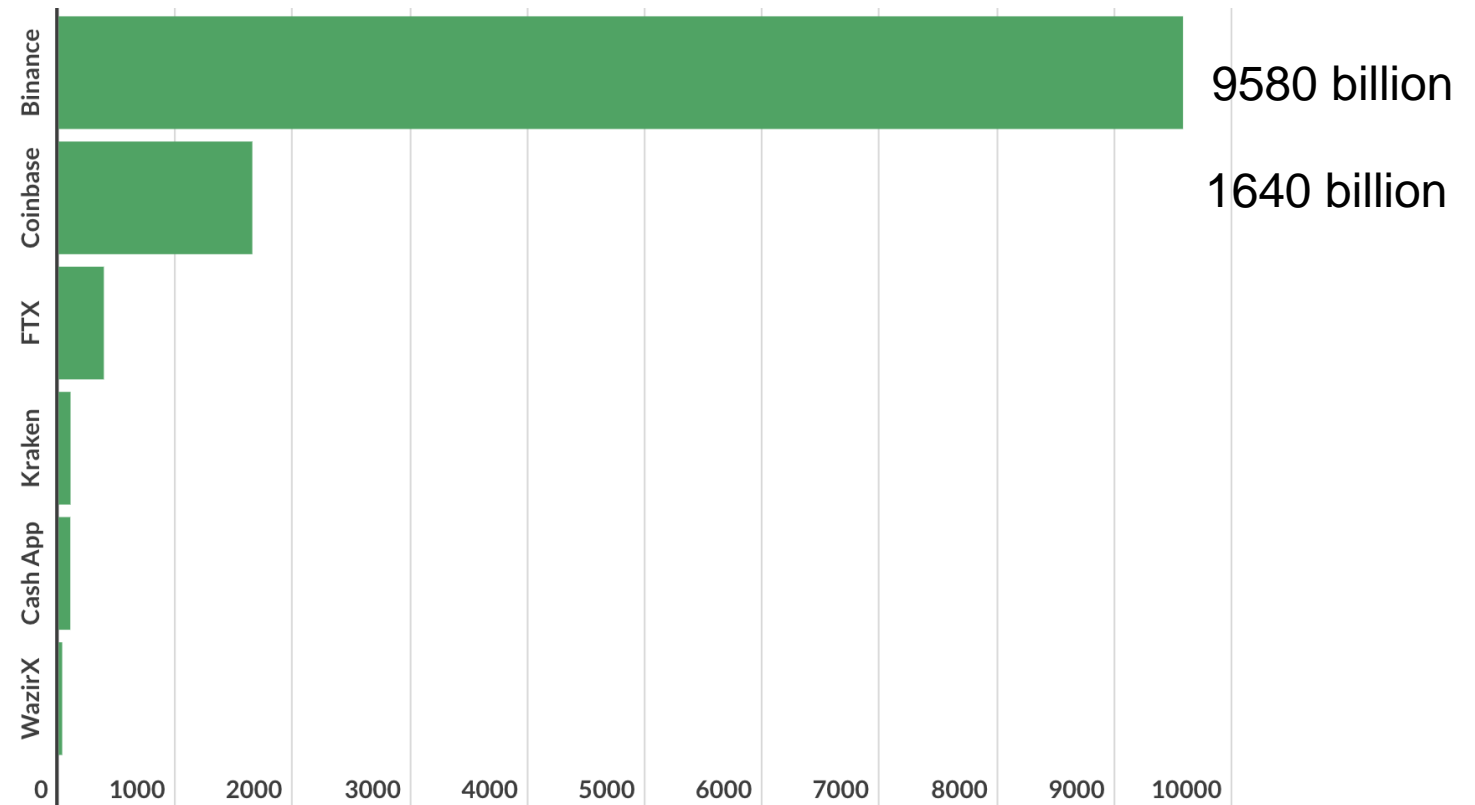
– Binance



– Coinbase



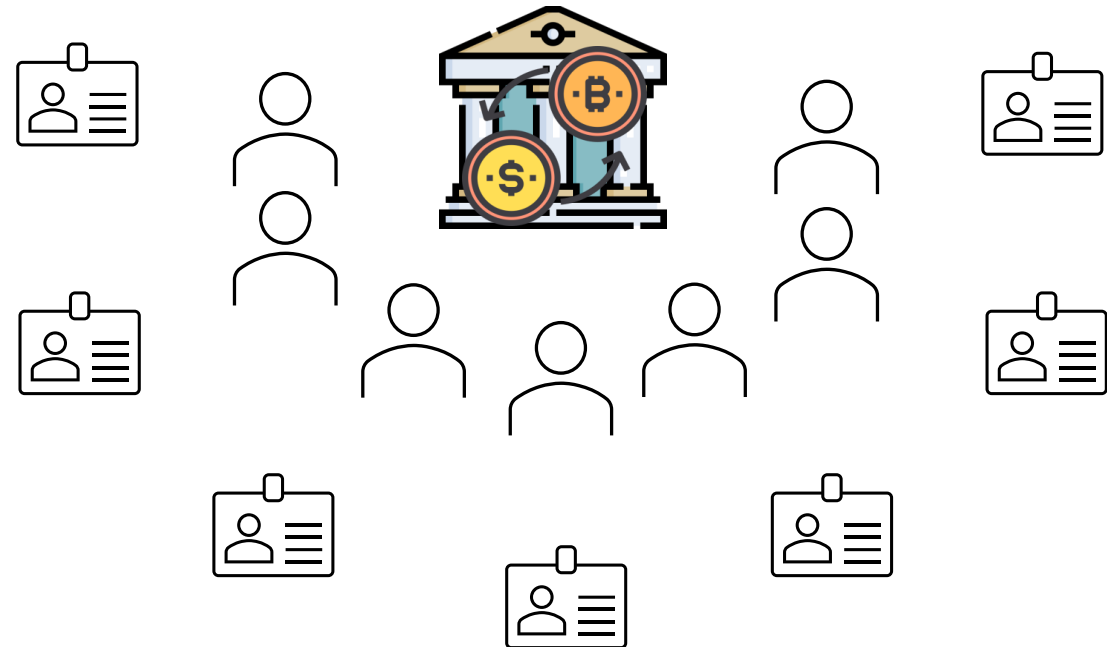
2021 Annual Trading Volume (USD)



# Background

## Centralized exchange platforms

- Register
- Deposit
- Exchange  
(include buy and sell)
- Withdraw
- File tax



# Background

## Compliance rules

KYC

AML

## Create a Coinbase account



! Always check that automated emails are coming from 'no-reply@coinbase.com' or another [valid Coinbase email address](#). Do not reply to or click on any links in emails without a valid address to complete your account setup.

### Get started

To invest, trade, and store [supported cryptocurrencies](#) on Coinbase, as well as do much more, get started here. For more information on all the services available in Coinbase supported countries, visit the [Supported Countries](#) page.

### What you'll need

- Be at least 18 years old (we'll ask for proof)
- A [government-issued photo ID](#) (we don't accept passport cards)
- A computer or smartphone connected to the internet
- A [phone number connected to your smartphone](#) (we'll send SMS text messages)
- The latest version of your browser (we recommend Chrome), or the latest Coinbase App version. If you're using the Coinbase app, make sure your phone's operating system is up-to-date.

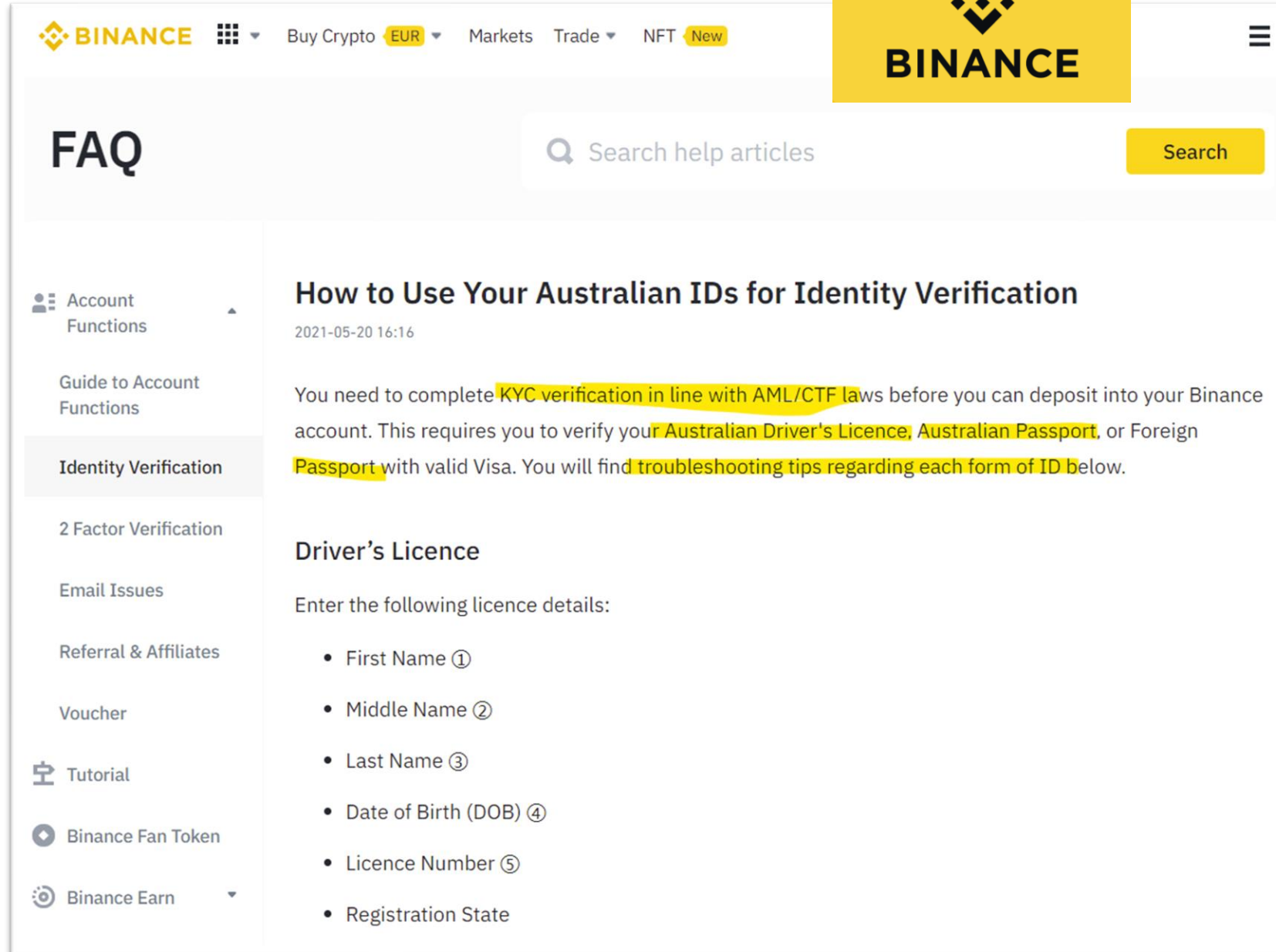
Coinbase doesn't charge a fee to create or maintain your Coinbase account. Learn about [pricing and fees](#).

# Background

## Compliance rules

KYC

AML



The screenshot shows the Binance website's FAQ section. The top navigation bar includes the Binance logo, a menu icon, and links for 'Buy Crypto', 'Markets', 'Trade', and 'NFT'. A search bar is located on the right. The main content area features a sidebar with categories like 'Account Functions', 'Tutorial', and 'Binance Earn'. The selected article is 'How to Use Your Australian IDs for Identity Verification', dated 2021-05-20. The article text states that users must complete KYC verification in line with AML/CTF laws before depositing. It lists acceptable IDs: Australian Driver's Licence, Australian Passport, or Foreign Passport with valid Visa. A section titled 'Driver's Licence' lists the required details: First Name, Middle Name, Last Name, Date of Birth (DOB), Licence Number, and Registration State.

**FAQ**

Search help articles

Search

**Account Functions**

Guide to Account Functions

**Identity Verification**

2 Factor Verification

Email Issues

Referral & Affiliates

Voucher

**Tutorial**

Binance Fan Token

Binance Earn

### How to Use Your Australian IDs for Identity Verification

2021-05-20 16:16

You need to complete **KYC verification in line with AML/CTF laws** before you can deposit into your Binance account. This requires you to verify your **Australian Driver's Licence, Australian Passport,** or **Foreign Passport** with valid Visa. You will find **troubleshooting tips regarding each form of ID** below.

#### Driver's Licence

Enter the following licence details:

- First Name ①
- Middle Name ②
- Last Name ③
- Date of Birth (DOB) ④
- Licence Number ⑤
- Registration State



# Background

## Compliance rules

KYC

AML

**Tax report**



## Understanding Coinbase taxes

For the 2021 tax year, US customers can use [Coinbase Taxes](#) to find everything needed to file Coinbase.com taxes. Coinbase Taxes will help you understand what Coinbase.com activity is taxable, your gains or losses, earned income on Coinbase, and the information and reports (including IRS forms) you need to file.

Check out our frequently asked questions found within the Coinbase Taxes Summary section for more information.

**Important:** Non-US customers won't receive any forms from Coinbase and must utilize their [transaction history report](#) to fulfill their local tax obligations.

Discover more about crypto taxes on Coinbase Learn:

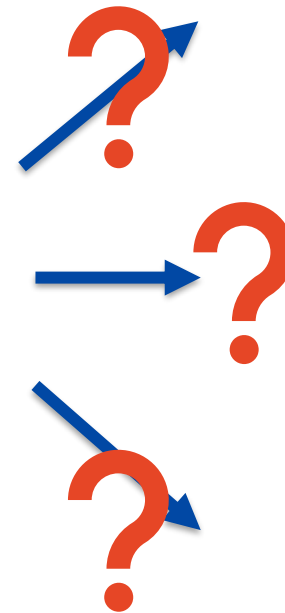
- [Understanding crypto taxes](#)
- [Tax forms, explained: A guide to U.S. tax forms and crypto reports](#)
- [Capital gains tax: What is it and how it applies to your crypto](#)
- [What is income: A guide to income and how it's taxed](#)

Below you'll find helpful information about including your Coinbase.com activity in your taxes.

# Privacy issue

## Conventional financial platform

- Bank
- Withdraw cash
- Privacy



# Privacy issue

## Cryptocurrency exchange platform

Register



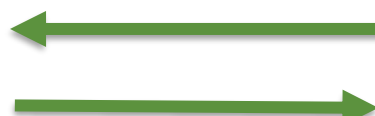
Real identity



Withdraw



Withdraw 10 BTC,  
wallet address



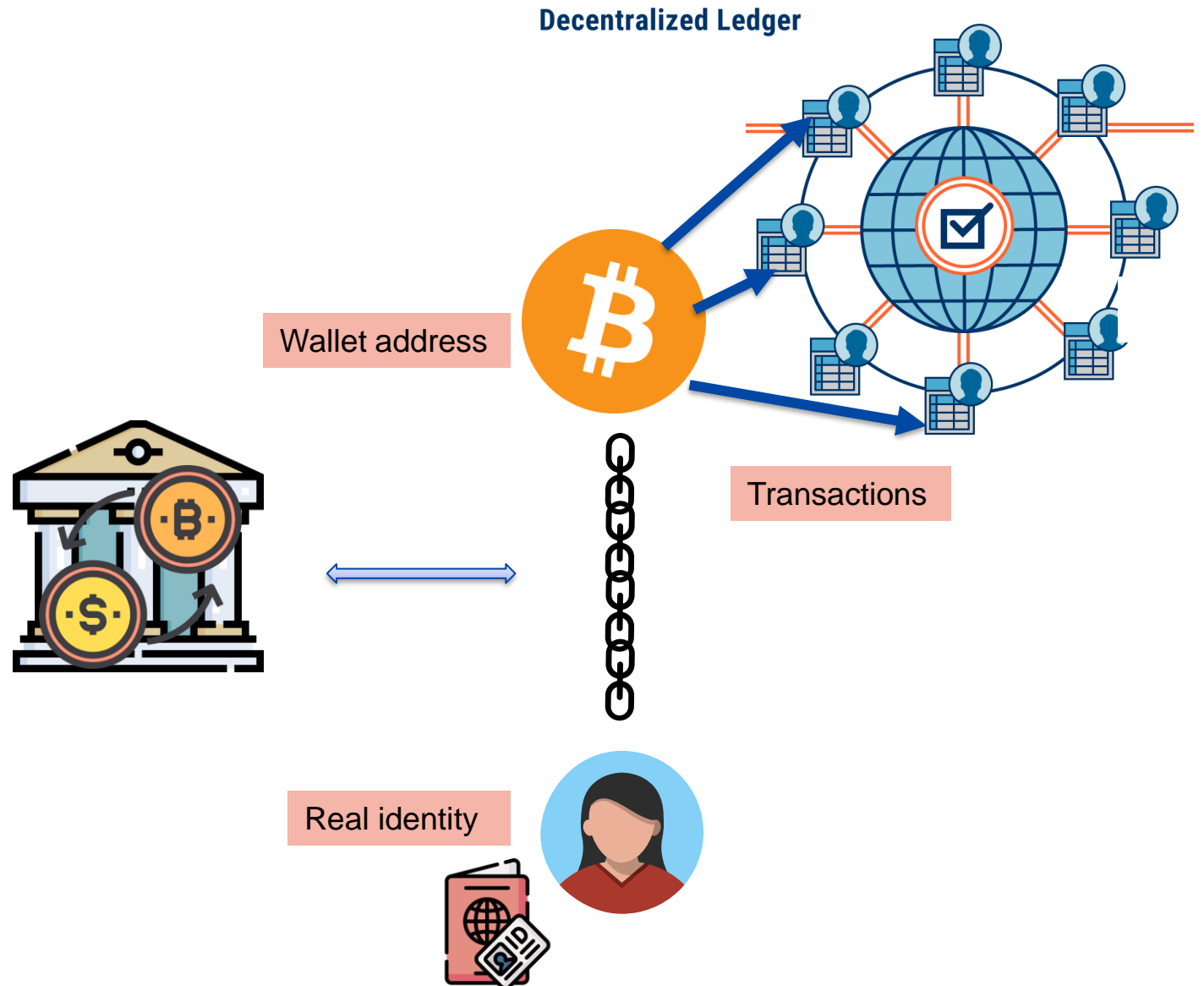
On-chain transaction



# Privacy issue

Privacy is violated!

- User's real identity
- Wallet address
- Identify all future transactions



# Our goals

- Overdraft prevention
  - Users cannot get more asset than they own
- Anonymity:
  - The platform cannot link the user's real identities with their wallet addresses
- Compliance:
  - Users must comply with all the regulation rules
  - Platform can do self-check to ensure it has enough asset

# Main challenges

Intuitive idea – basic anonymity

- Only focus on the withdraw operation



# Main challenges

## Basic anonymity limitation

- Platform knows the asset state of each user
- The anonymity set is small



??? withdraw 99 ETH

Must be Bob

- Only hide withdrawal identity
- Can we hide all information?

# Main challenges

## Towards full anonymity

- Simple example:
  - Registered users: Alice, Bob, Clare
  - David joins, Ella Joins
  - David deposits 5 BTC
  - Alice exchanges 5 BTC to 10 ETH
  - Alice withdraws 10 XRP



# Main challenges

## Towards full anonymity

- Simple example:
  - Registered users: Alice, Bob, Clare
  - **David** joins, **Ella** Joins
  - David deposits **5 BTC**
  - Alice exchanges 5 BTC to 10 ETH
  - Alice withdraws **10 XRP to address1**

**Unavoidable  
leakage**

# Main challenges

## Towards full anonymity

– Simple example:

- Registered users: Alice, Bob, Clare
- David joins, Ella Joins
- **David** deposits 5 BTC, Ella does nothing
- **Alice** exchanges **5 BTC to 10 ETH**
- **Alice** withdraws 10 XRP



- **XXX** deposits 5 BTC
- **XXX** exchanges **XXX** to **XXX**
- **XXX** withdraws 10 XRP



Could be  
Alice, Bob, Clare,  
David, Ella

# Main challenges

## Full anonymity with Compliance

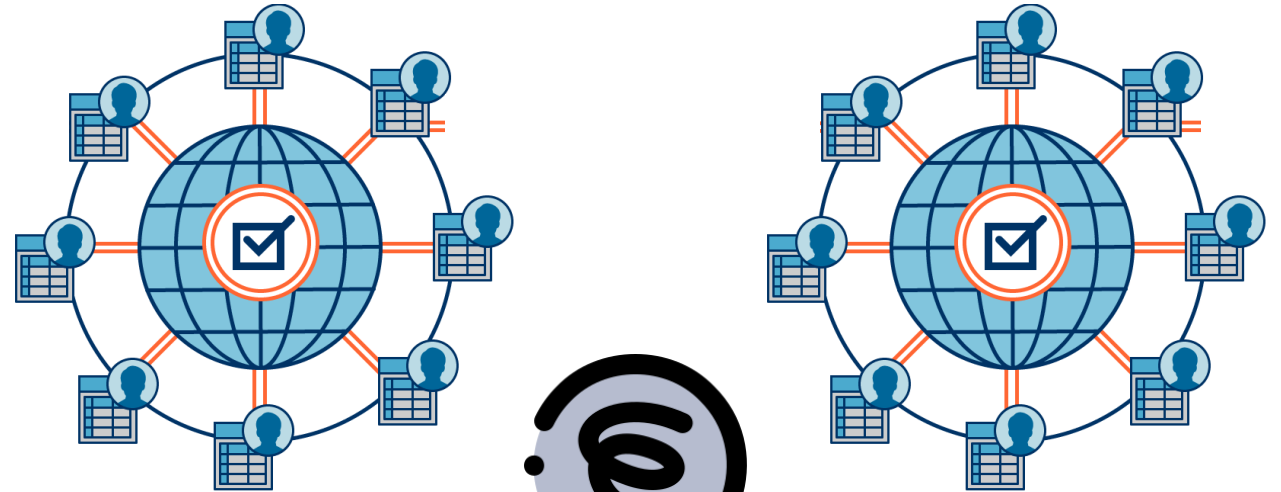
- **KYC**: Real name registration
- **AML**: Malicious address detection
- **Tax report**
  - Privacy requirement hinders computing the accumulated profit directly
  - Cannot link the selling price with the buying price
  - Cannot link one user's transactions together

# Modeling

## Full anonymity

### Interaction indistinguishability

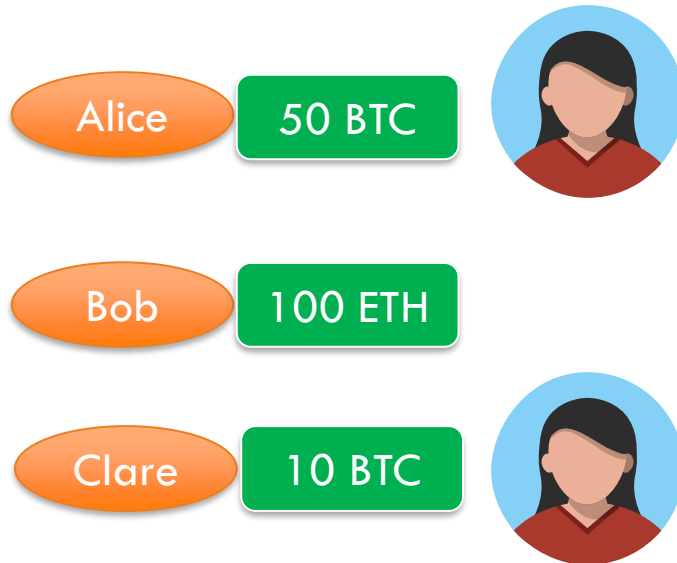
- Simulate two worlds
- Interact with different queries
- Same unavoidable leakages
- Cannot distinguish



Adversary A  
(the platform)

# Our construction (Basic anonymity)

Withdraw



# Our construction (Basic anonymity)



Prepare: issue credential



$\text{Com}(\text{id}, \text{BTC}, 8)$

Proof of enough



Blind signature  $\sigma$

Unblind  $\sigma$  to  $\sigma^*$



$\text{Cred} = (\text{id}, \text{BTC}, 8, \sigma^*)$



Commitment

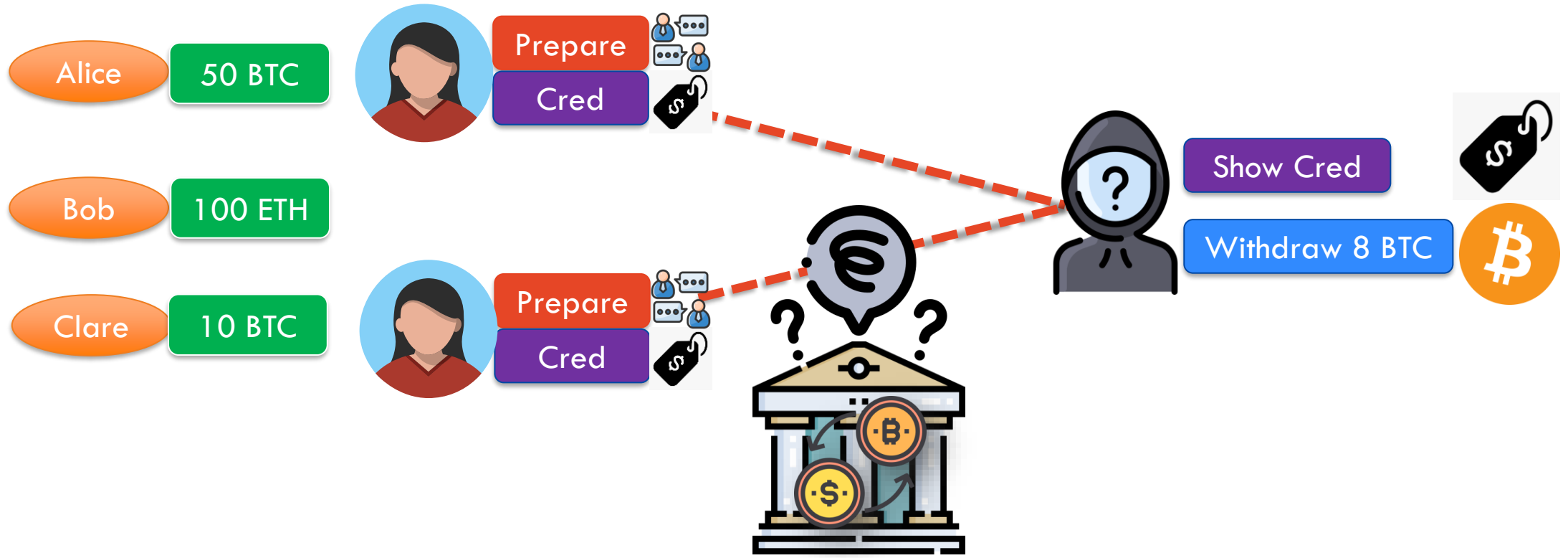
Zero-knowledge proof

Blind signature



# Our construction (Basic anonymity)

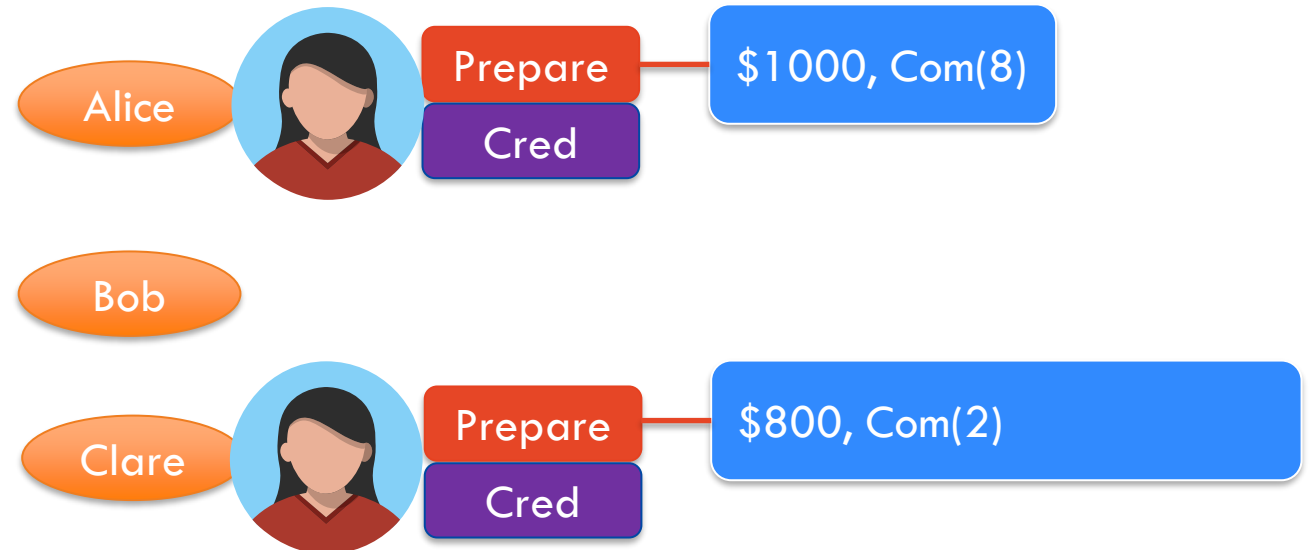
Withdraw



## Our construction (Basic anonymity)

### User compliance

- Prepare:
- Keep current asset price and withdrawn amount commitment in the user's account

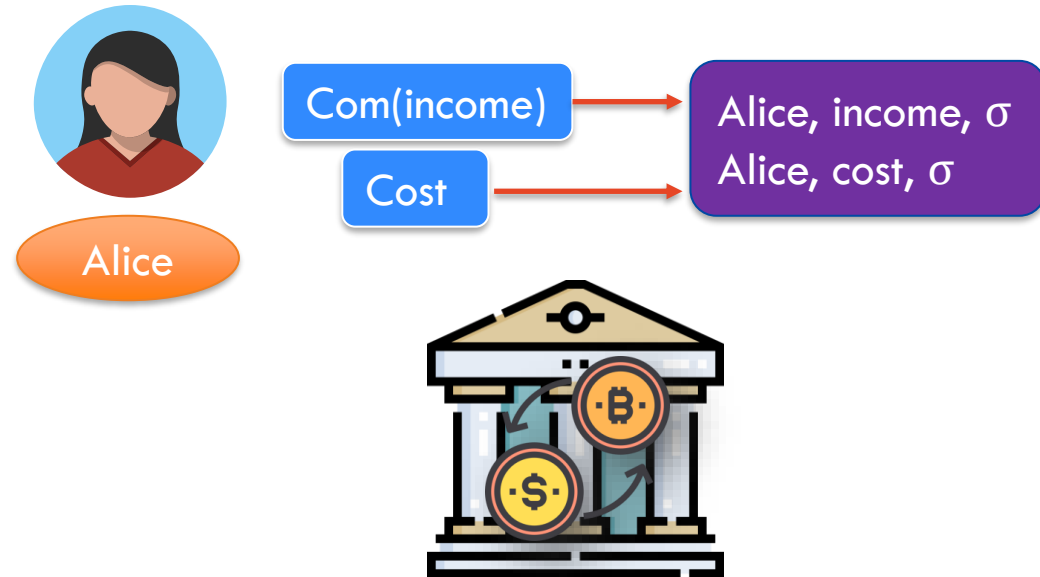




# Our construction (Basic anonymity)

## User compliance

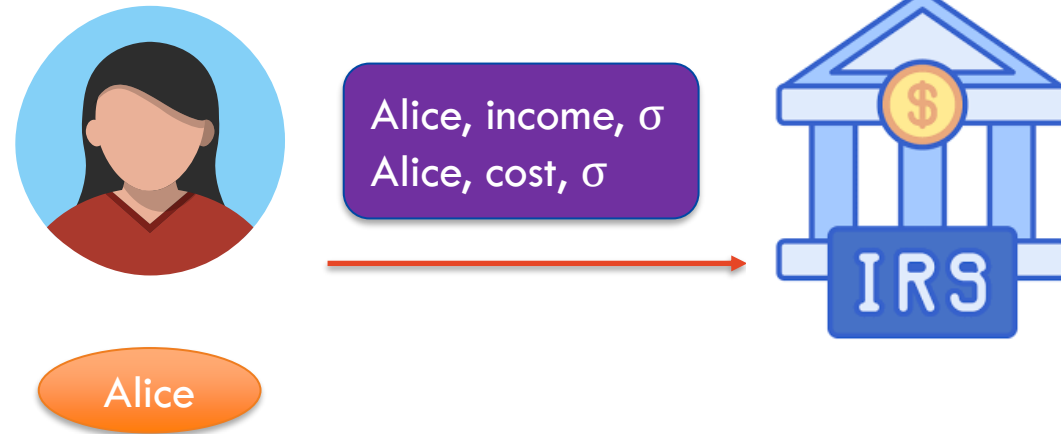
- Compute the accumulated gain commitment
- Request a blind signature on the committed accumulated gain
- Request a signature on the accumulated cost



## Our construction (Basic anonymity)

### User compliance

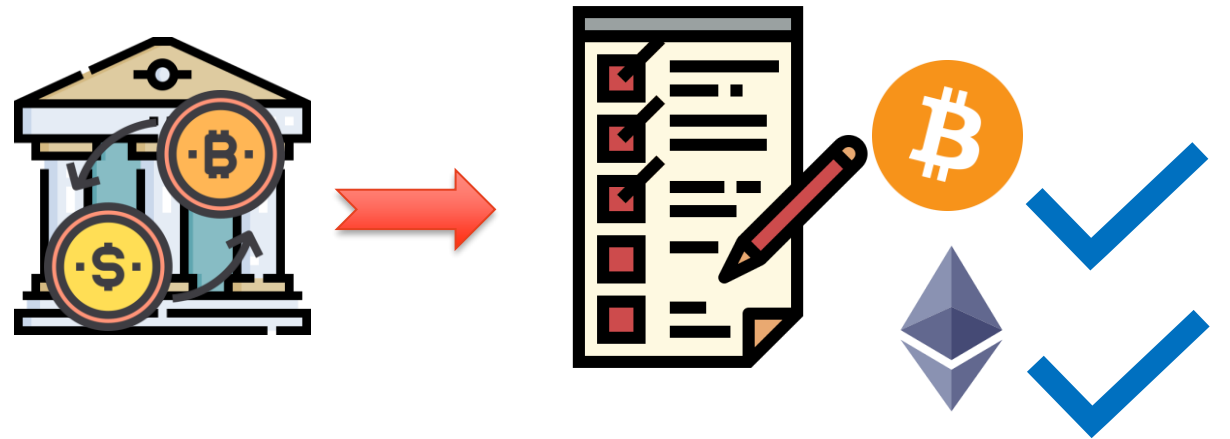
- Send the authenticated gain and cost to the authority



## Our construction (Basic anonymity)

### Platform compliance

- The platform knows the total amount of each asset, so it can do the self-check to ensure it has enough asset for withdrawal.



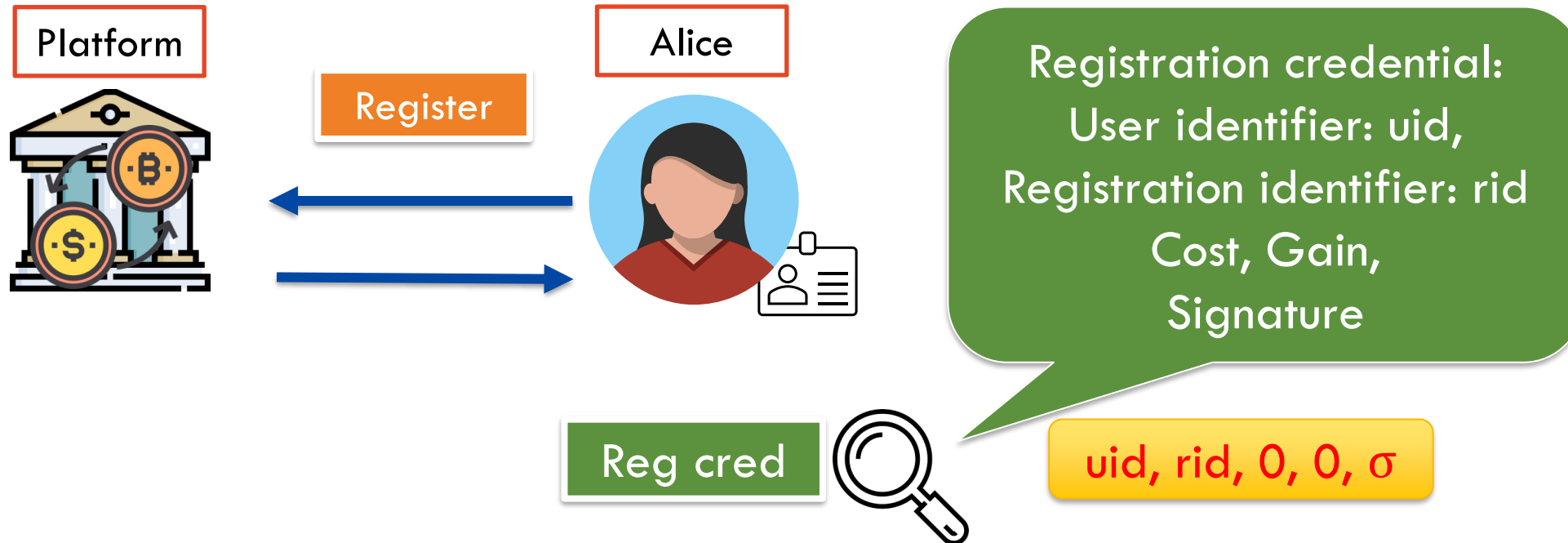
# Our construction (Full anonymity)

## High level idea

- Cut the link from Register to Withdraw
- Make all interactions anonymous and private
- Technique: Expand Zero-knowledge proof

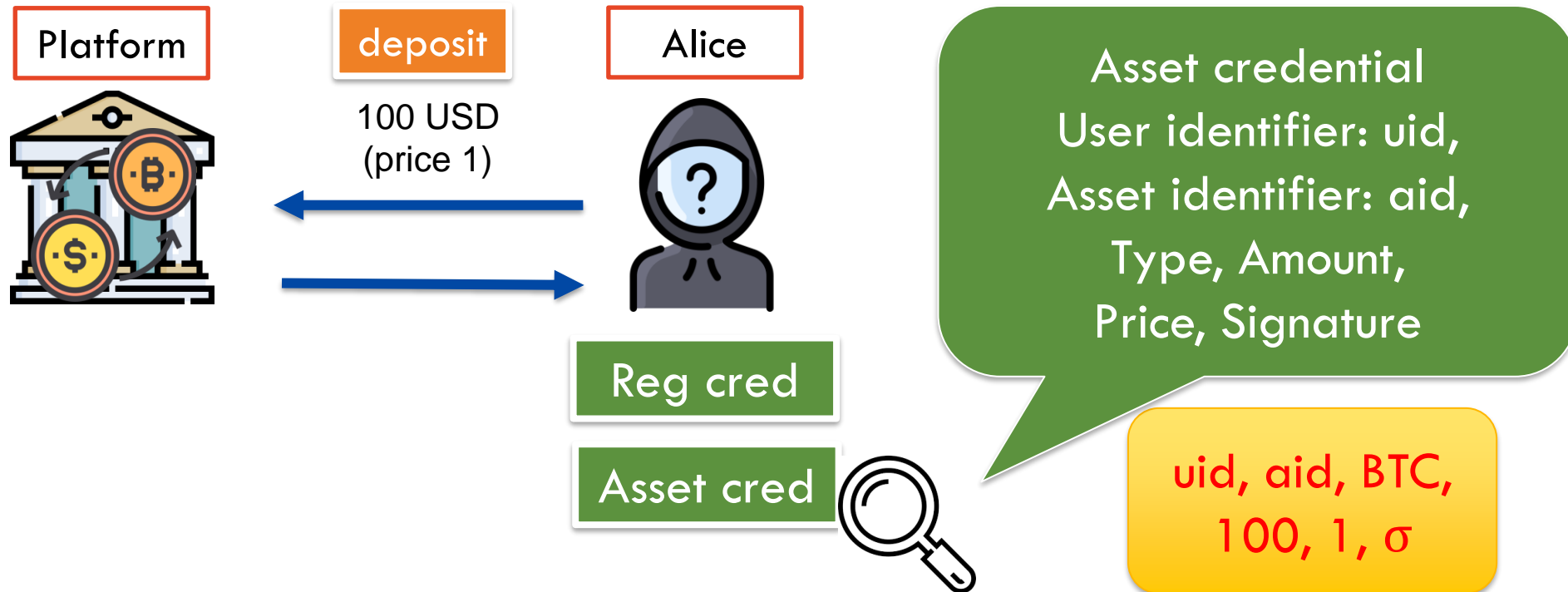
# Our construction (Full anonymity)

## Registration

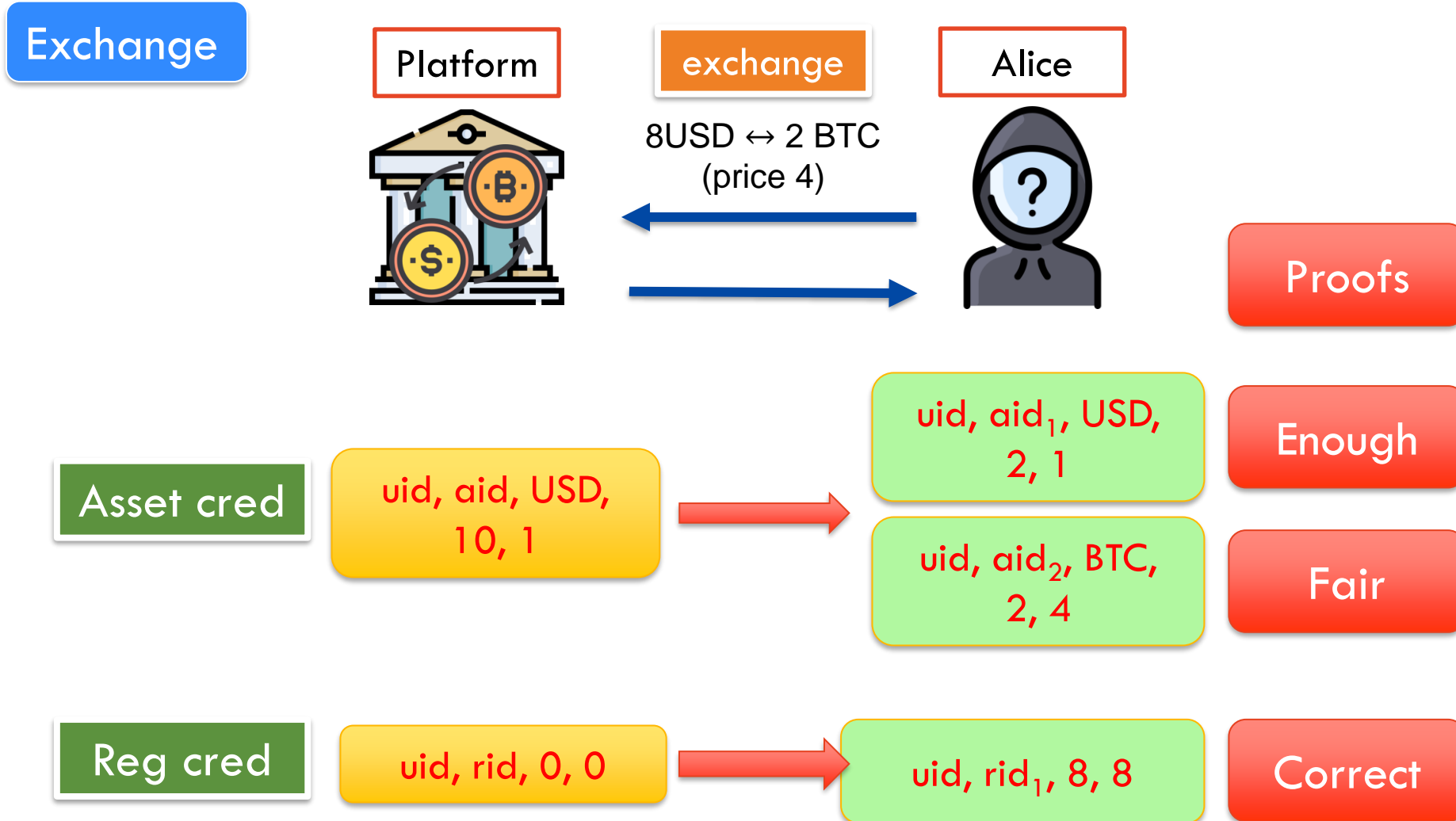


# Our construction (Full anonymity)

## Deposit



# Our construction (Full anonymity)



# Our construction (Full anonymity)

Efficient fairness proof

uid, aid<sub>2</sub>, BTC,  
2, 4

Fair

$$8 * 1 = 2 * 4$$



# Our construction (Full anonymity)

Efficient fairness proof

uid, aid<sub>2</sub>, BTC,  
~~2, 4~~

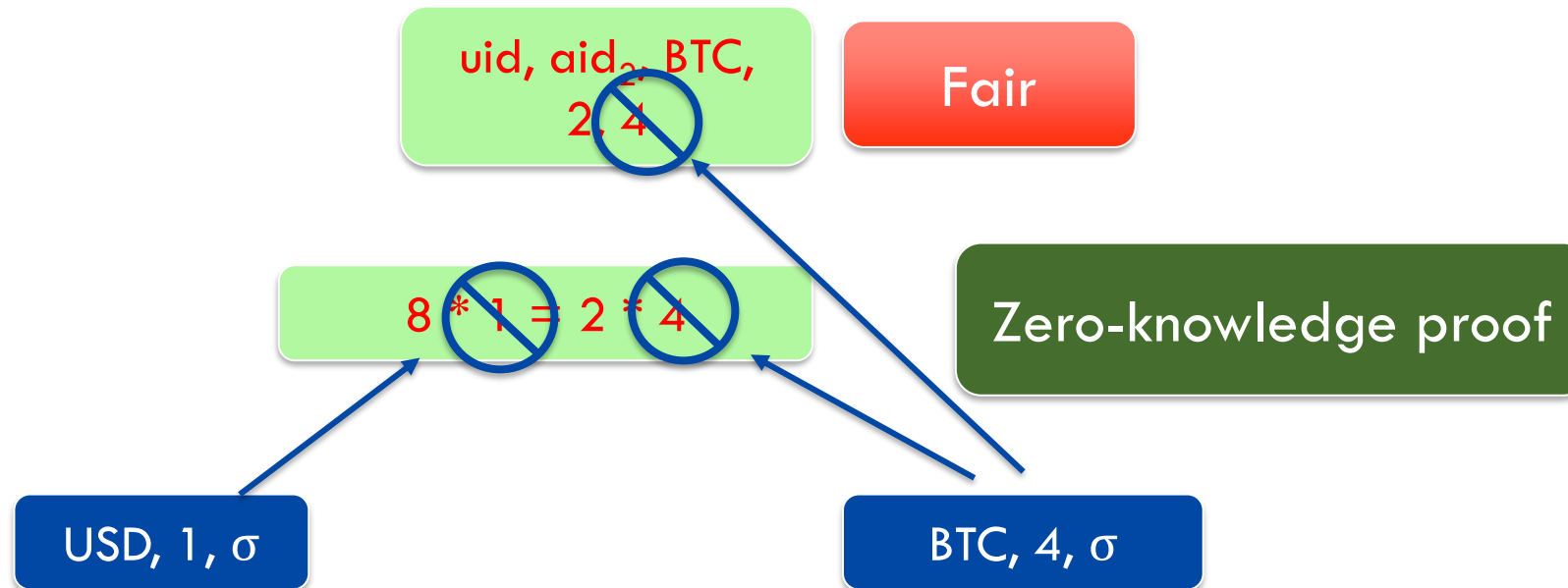
Fair

~~8 \* 1~~ = ~~2 \* 4~~

- Hide which prices are used
- One-out-of-many proof ? ?
- $\log(n)$  communication cost
- $O(n)$  computation cost
- Inefficient!

# Our construction (Full anonymity)

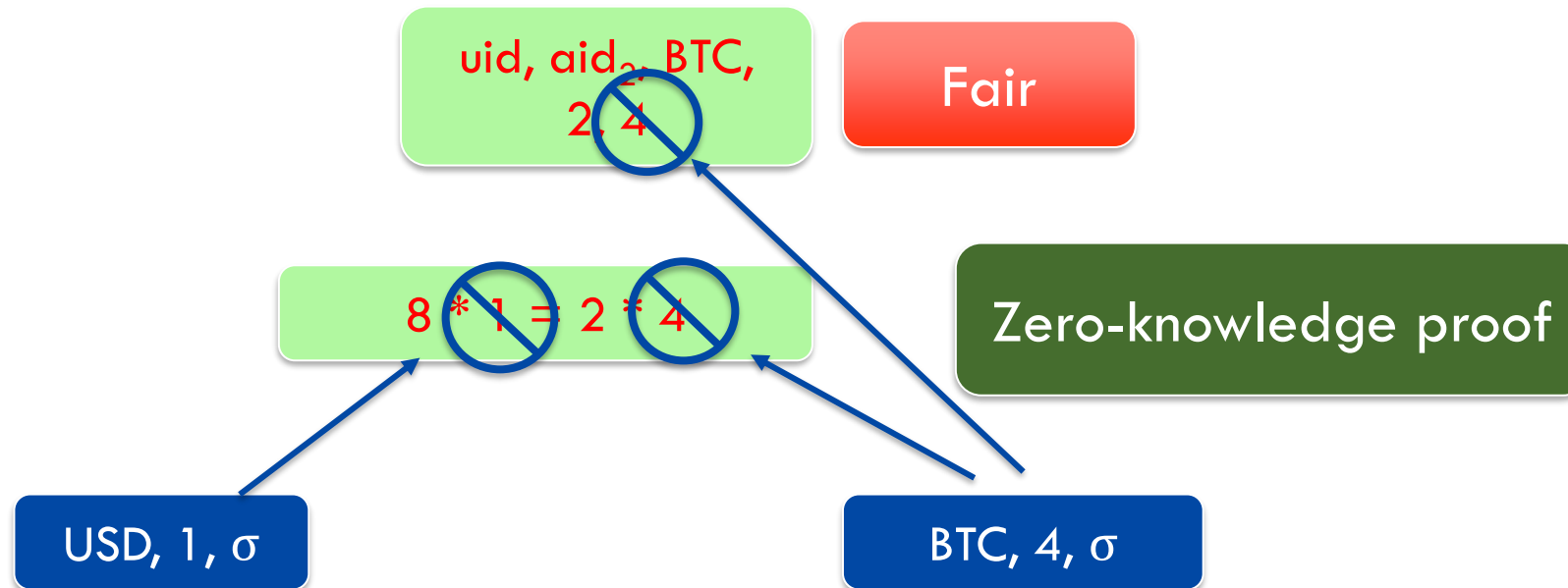
Efficient fairness proof



- Platform issue credential on each price
- Prove the used type and price are equal to the chosen one

# Our construction (Full anonymity)

Efficient fairness proof

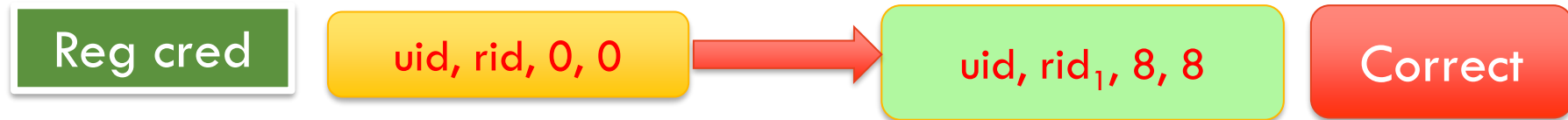


- Constant communication cost
- Constant computation cost

Reduce the cost of proof to constant

# Our construction (Full anonymity)

Correctness proof for compliance



Add Cost, Gain on Reg cred correctly

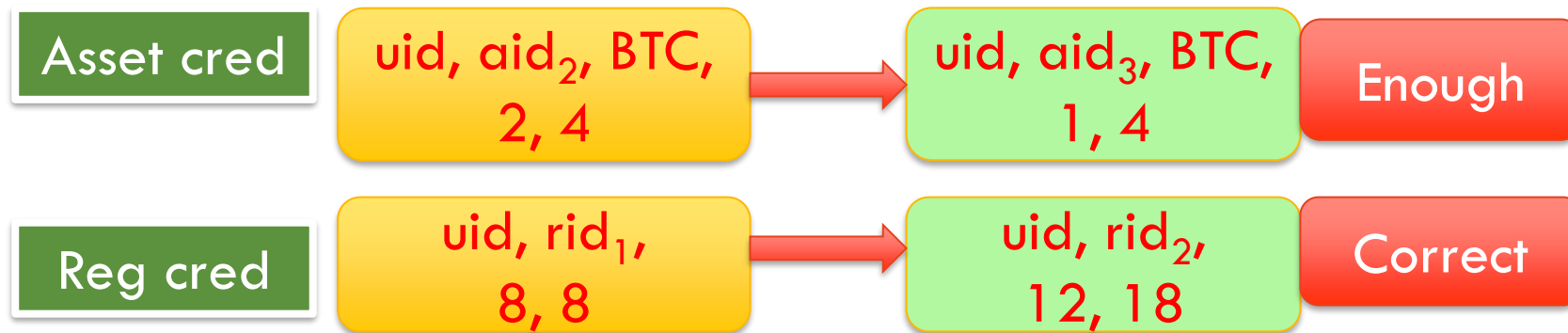
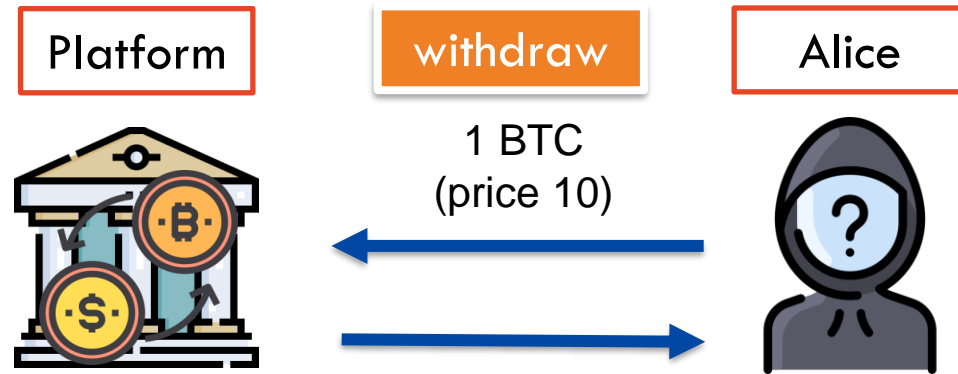
$$\text{New Cost} = 0 + 8 * 1$$

$$\text{New Gain} = 0 + 2 * 4$$



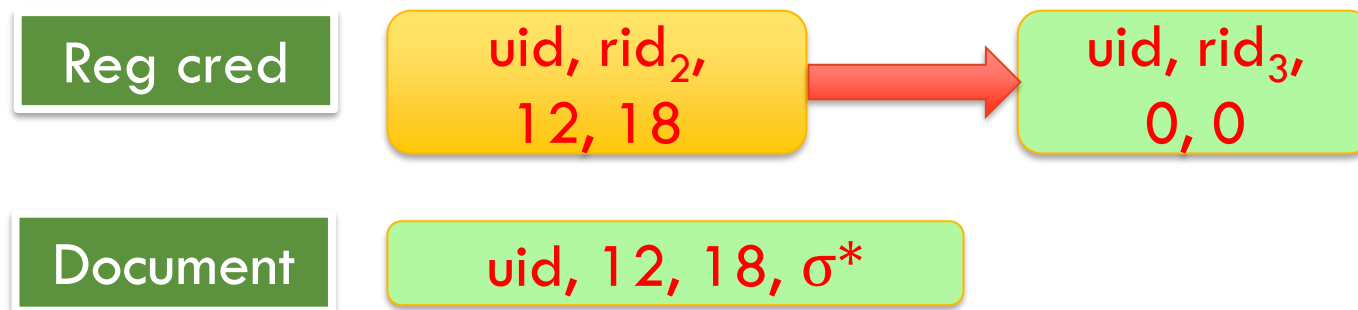
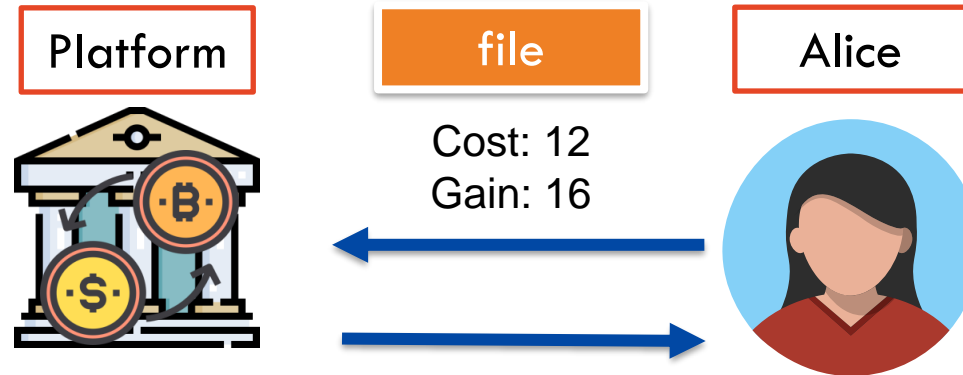
# Our construction (Full anonymity)

## Withdrawal



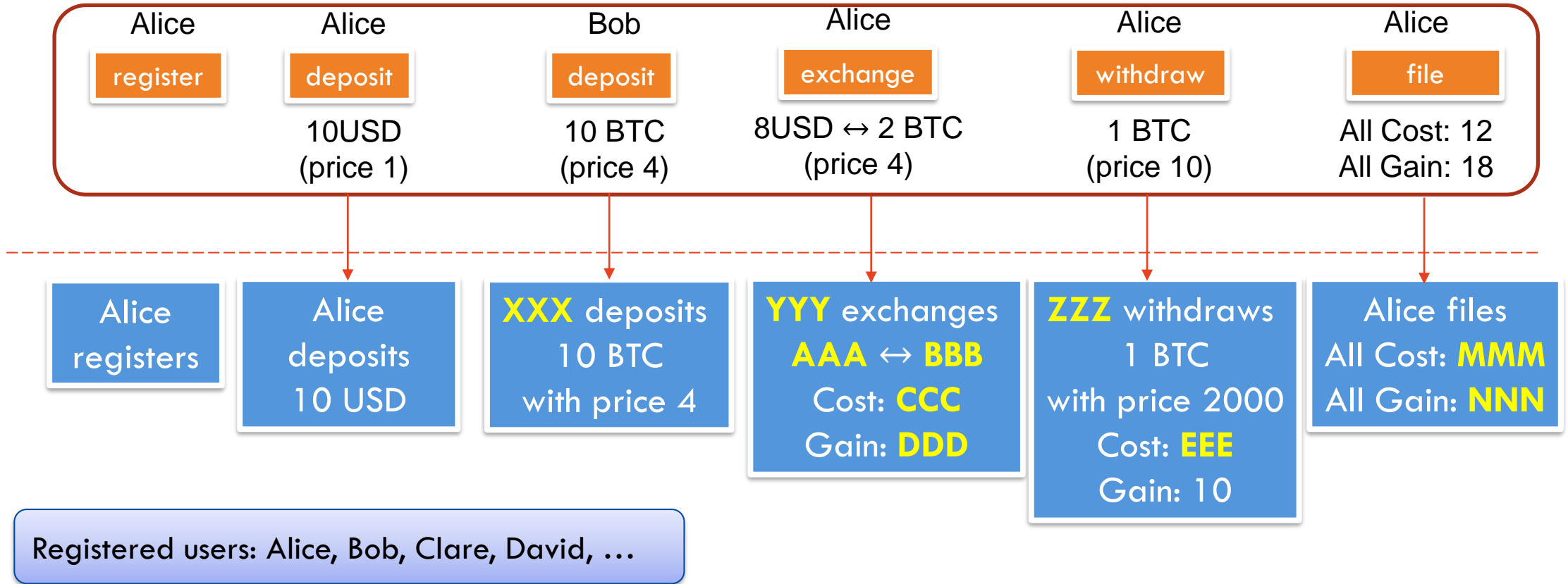
# Our construction (Full anonymity)

File



# Our construction (Full anonymity)

## Platform's view



## Our results

### Private and compliant cryptocurrency exchange

- Overdraft prevention
- Basic anonymity/ Full anonymity
- Compliance



# Our results

## Performance

- Computation cost for each procedure is **less than 88ms**
- Communication cost of each procedure is **less than 12kb**
- **Practical enough**

Table 1: Computation cost in milliseconds

Party	Join	Deposit	Exchange	Withdraw
Pisces-user	9	11	46	37
Pisces-platform	7	14	88	62

Table 2: Communication cost in kilobytes

Party	Join	Deposit	Exchange	Withdraw
Pisces-user	2.6	3.3	12	8.7
Pisces-platform	1.8	1.8	2.3	2.8

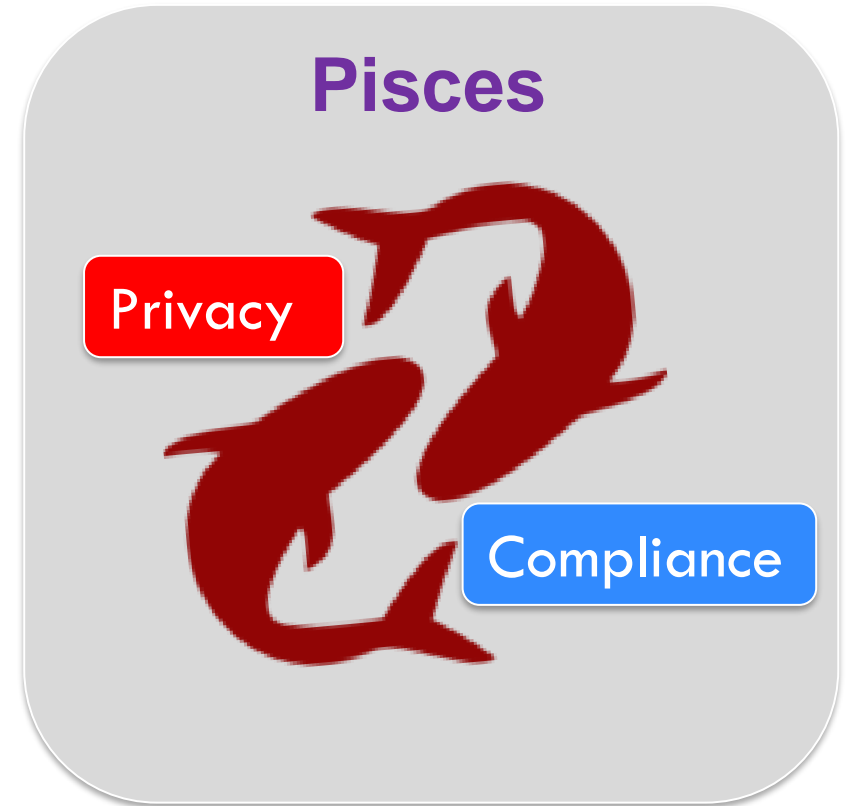
# Open problem

## Solvency issue

- All exchange details should be hidden
- Withdraw a large amount of certain asset
- Our Pisces can achieve liquidity requirement
- A more rigorous solution remains open
  - Keep sufficient reserve and liquidity

## Take away

- The cryptocurrency exchange platform serves as the vital link between the real world and the realm of crypto. However, this junction often compromises users' privacy.
- Preserving privacy may appear at odds with regulatory compliance. Our research demonstrates their compatibility. We aim to safeguard the privacy of honest users while actively thwarting illicit activities.



*Thank you!*  
*Any questions?*

<https://eprint.iacr.org/2023/1317>

<https://github.com/yananli117/Pisces>

