SudoCash: A Peer to Peer Digital Non-Centralised IOU System

Abhimanyu M A

March 2017

Abstract

The paper describes a digital non-centralised system to create and maintain a record of IOU for inter-personal transactions in a trusted network. The current Indian government is making a massive push towards digital economy. However digital transactions still are not well suited for low value transactions, and also have immense privacy concerns.
Given that India has robust trust based communities, especially in rural areas, we propose a system whereby users can exchange IOU(I Owe yoU) in lieu of actual currency. The system is very privacy concious with minimal (and if required zero) information leakage outside of the two people involved in a transaction.
The system uses Digital Signatures to create digitally signed IOU records, and create a trail of IOUs from each person, and effectively allows the issuer of the IOU to act as a bank.

1 Introduction

The world is moving towards digital currency however there are definite flaws with the system.

1. Cost of transaction for small value transactions is significant.
2. Centralised systems with loss of privacy
3. Lack of Open Source Alternatives
4. Need for internet connectivity

2 Mechanisms

2.1 Currency

Given that the aim of the system is to elevate regular population to being able to "become banks" we allow the users to issues IOUs in the following set of currencies.

Standard Currency This is built into the system and are the set of standard currencies that are in use across the world and whose definitions are agreed upon by EVERYBODY in the system. It includes all the standard currencies used by governments like US Dollar, Euro, non-governmental currencies like Bitcoin, and certain agreed upon items like grammes of 24ct gold.

Private Pegged Currency This is a currency that is defined by an individual and that reguires the currency definition to include what the currency is pegged to. It need not be pegged to standard currencies, but can even contain non-standard items like "1 Hour of my effort". It is the responsibility of the person recieving a IOU note in such a currency to ensure that they understand and value the currency. The only person who can issue a IOU note in this particular currency is the person who has defined that currency (except for cancellation IOUs)

Public Pegged Currency This is a currency that is equivalent to the previous one, but allows people other than the original creator of the currency to issue IOU in that particular currency.

We will in future have two more currencies the *Private Floating Currency* and *Public Floating Currency* that is not pegged to anything, and varies based on supply and demand principles just like regular fiat currencies worldwide. However they are currently not supported by the specification.

2.2 Transactions

The base unit in any transaction is an $IOURecord$ defined as R henceforth. It contains two fields, the data field and a signature field, this allows more signatures to be appended to a transaction as a form of verification. The data field gives details of the transaction. We currently have the following transaction types, with possibily more types that can be described later.

IOU This is the most common and default record, and merely records that *Alice* owes *Bob* an amount as mentioned in it, in the currency as mentioned in it. This record needs to be necessarily signed by *Alice* and optionally signed by *Bob*.

Cancellation This references an *IOU* already issued, and has to be signed by both the parties, and effectively cancels the previous *IOU* issued. This is mathematically equivalent to issuing a *IOU* of the same amount in reverse, but we make a seperate one because of the currency issue.

Settlement This is a special transaction which is used to collapse multiple transactions into a single one, and is mathematically effective to removing all previous *IOU* where each party may have given to the other, and replacing all the previous *IOU* of a single currency

The following are examples of a transaction

```
transaction = {
  "data": {
    "nonce_id": "k9AD-23_",
    "amount": 2342.23,
    "currency": "INR",
    "base_amount": 234223,
    "type": "IOU",
    "debtor_fingerprint": "DE32 F82D B32D 9898"
    "creditor_fingerprint": "32FF 6321 AD66 212C"
  },
  "signatures": [
    {
      "method" : "RSA",
      "strength": "2048",
      "fingerprint: "DE32 F82D B32D 9898"
      "signature": <Signature>,
      "type": "PRIMARY"
    },
    {
      "method" : "RSA",
      "strength": "2048",
      "fingerprint: "32FF 6321 AD66 212C"
      "signature": <Signature>,
      "type": "SECONDARY",
    },
```

```
  ]
}
```