DecentralizedDebit

Gabriel Ruoff,
geruoff@syr.edu

Abstract

Since the advent of Bitcoin in 2009, decentralized digital currencies have slowly made their way into mainstream social, political, and financial circles. Recently, large corporations such as Tesla Motors have bought into cryptocurrency markets in staggering amounts. Large banks, such as J.P. Morgan and Goldman Sachs, have issued RFI's[1] with the intention of developing investment strategies relating to digital assets[2]. Even BlackRock, the worst largest asset manager, has been transparent about entering the crypto space[3]. *As corporations and financial institutions continue to embrace cryptocurrency as a viable store of value, and retail investors continue to accumulate digital assets, there will, without a doubt, be high demand for the development of public physical and digital 'crypto-commerce' infrastructure.* So where is this infrastructure? As of now, the greatest argument against the viability of cryptocurrency is that the fee structures of popular assets are not suited for small and frequent transactions[4], or commonly put, 'Bitcoin can't buy you a cup of coffee'. This project serves as a counter-argument to this long-held idea. By utilizing a centralized cryptocurrency payment processing service, the fee structure of cryptographic assets can be leveraged to offer the public low-overhead, high-frequency payment options while preserving their individual anonymity and digital security to the same degree that the underlying digital asset provides.

Structure

This infrastructure, further referred to as 'The Service' consists of three systems which cater to two usage groups who are assumed to hold an account on The Service: customers and merchants. A *customer* is an individual who intends to exchange currency with a *merchant* who provides them with goods or services. The first system is the *central server* which stores and processes data. This central server communicates with the other two systems, the *merchant-side* and *customer-side* over the internet using an API[5]. The customer-side system allows customers to interact with the central server to manage their user account[6], while the

---

[1] Requests for Information
[2] https://www.coindesk.com/goldman-sachs-to-enter-crypto-market-soon-with-custody-play-source
[3] https://markets.businessinsider.com/currencies/news/blackrock-begun-dabble-bitcoin-investors-hunting-value-boss-rick-rieder-2021-2-1030096330
[4] https://www.biznews.com/global-investing/2021/02/10/bitcoin-cant-replace-cash-yet
[5] Application Programming Interface
[6] I.e. manage individual wallets, deposit funds, etc..

merchant-side system allows merchants to submit transactions to the central server. These concepts are illustrated in the following list and flow-chart.

Usage groups:
- Customer - individual who purchases an item or service.
- Merchant - individual who exchanges goods and services for payment.
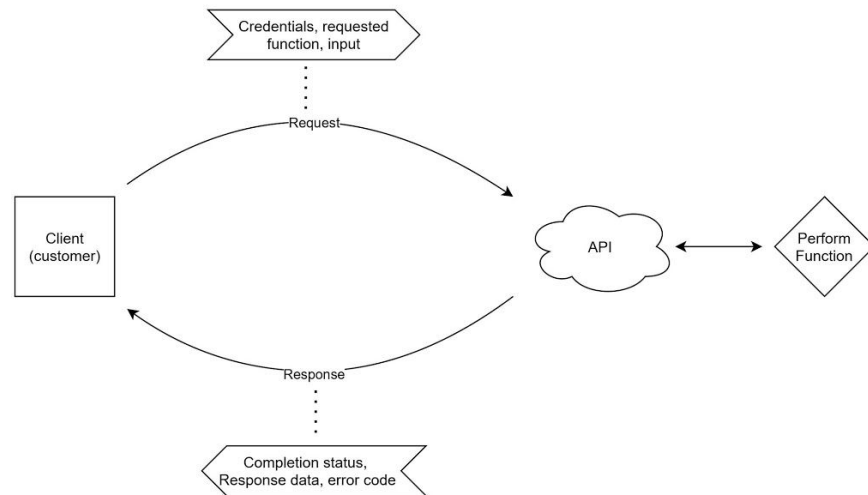
Systems:
- Central server
    - Manages data for The Service
    - Handles API calls
    - Processes transactions
- Merchant-side
    - Submits transactions to the central server
- Customer-side
    - Interacts with the central server and provides account management to the customer
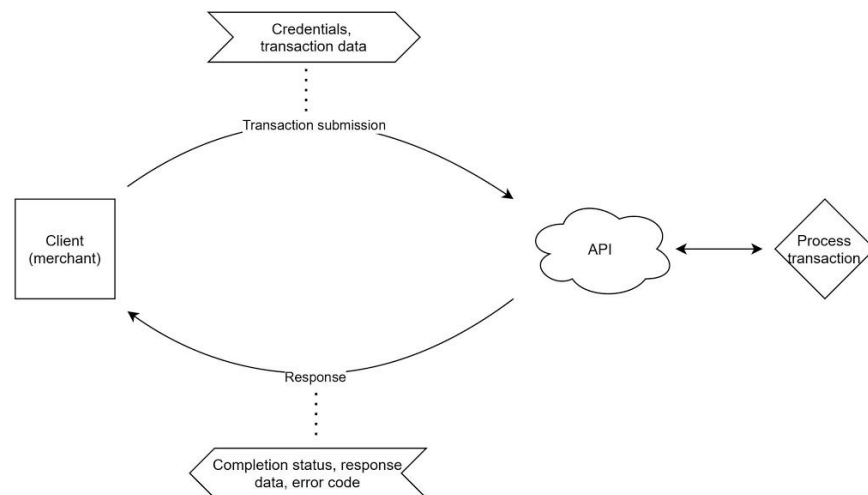
DecentralizedDebit API - API Call Overview

Gabriel Ruoff, geruoff@syr.edu

Customer-API interaction

```
                    ┌──────────────────────┐
                    │ Credentials, requested│
                    │   function, input     │
                    └──────────────────────┘
                              ┊
                           Request
            ┌─────────┐                    ╭──────╮         ◇
            │ Client  │                    │  API │ ◄────► Perform
            │(customer)│                   ╰──────╯        Function
            └─────────┘
                           Response
                              ┊
                    ┌──────────────────────┐
                    │  Completion status,   │
                    │ Response data, error code│
                    └──────────────────────┘
```

Merchant-API interaction

```
                    ┌──────────────────────┐
                    │   Credentials,        │
                    │  transaction data     │
                    └──────────────────────┘
                              ┊
                      Transaction submission
            ┌─────────┐                    ╭──────╮         ◇
            │ Client  │                    │  API │ ◄────► Process
            │(merchant)│                   ╰──────╯       transaction
            └─────────┘
                           Response
                              ┊
                    ┌──────────────────────┐
                    │ Completion status, response│
                    │    data, error code   │
                    └──────────────────────┘
```

Security

In any situation where a centralized entity is processing financial transactions on behalf of a user or merchant over a public protocol, such as HTTP[7], it is imperative that the privacy and interests of all users are protected. The Service uses a specialized key-based encryption

---

[7] Hyper-Text-Transfer-Protocol

process in order to ensure that illegitimate transactions can be easily recognized and discarded by the central server. Additionally, this encryption process ensures the anonymity of the customer, as it ensures no unencrypted user data may exist outside of The Service's database.