Plutus White Paper

Danial Daychopan
https://plutus.it

13 Dec 2015

Introduction

The Plutus Mobile Application enables a user to make contactless Bitcoin payments at any merchant with a Near Field Communication (NFC) enabled checkout terminal. This is the most practical way to pay with Bitcoin, because the payment process consists only of holding a mobile device above the merchant's NFC reader. As a result, Bitcoin payments are effectively accepted by proxy at over 32 million brick and mortar merchants around the world.

The primary purpose of Plutus is to provide incentive for, and enable, the practical day-to-day usage of Bitcoin; ultimately accelerating mass-consumer adoption.

The competitive advantage of Plutus, within the mobile payments industry, is the effective utilization of the rapidly expanding Ethereum network. Through a transparent and decentralized network protocol, underwritten by distributed ledger technology (the blockchain), Ethereum allows Plutus to deploy smart contracts to enable secure, peer-to-peer (P2P) exchange of fiat currency and Bitcoin, with the added benefit of automatic escrow. Using these methods, the Plutus Decentralized Exchange Network (PlutusDEX) of traders convert Bitcoin deposits into a prepaid debit balance that is valid at any contactless point-of-sale (POS) terminal.

The philosophy of the application itself is open, inclusive and committed to the network health and widespread usage of Bitcoin. As such, a public trading API will be available, and 3rd party development is encouraged.

1 The Ecosystem

Bitcoin merchant adoption has thus far proved to be a challenging endeavor. Merchants are hesitant to accept it, and users are unable to spend it. Because there is no widespread Bitcoin point-of-sale (POS) infrastructure currently in place, merchants often reconsider accepting Bitcoin due to its perceived complexity, which may increase labor costs in the short run, because of the extra employee training required. In many cases, they stop accepting Bitcoin or become frustrated with early technical difficulties. These difficulties often lead to narrowing merchant adoption of Bitcoin and the blockchain infrastructure in general. This creates a kind of chicken-and-the-egg problem, which contributes to forcing merchant-side Bitcoin payment processors to significantly limit their expansion and adoption efforts.

This is the crux of the problem which makes Plutus an optimal use case and ideal app for miners, entrepreneurs, freelancers and anyone else who earns Bitcoin. By avoiding the need to wait for merchant adoption, consumers immediately gain both local and international opportunities for spending the digital currency at physical locations. The Plutus ecosystem can be seen in Figure 1. The chicken-and-the-egg problem is solved through both increased user *and* merchant adoption, because of Plutus' vastly improved ease-of-use, lowered costs, and greater efficiency for merchants, in both the long run and the short run.

2 Overview & Process

Plutus relies heavily on distributed computing and incorporates connections to the Bitcoin and Ethereum networks, as well as the traditional debit card infrastructure. As such, it is a hybrid system with both centralized and decentralized network components.

The structure of the Plutus Internal Infrastructure (Figure 2) relies on several interconnected servers and modules. The mobile app itself connects via Secure Sockets Layer (SSL) end-to-end encryption to

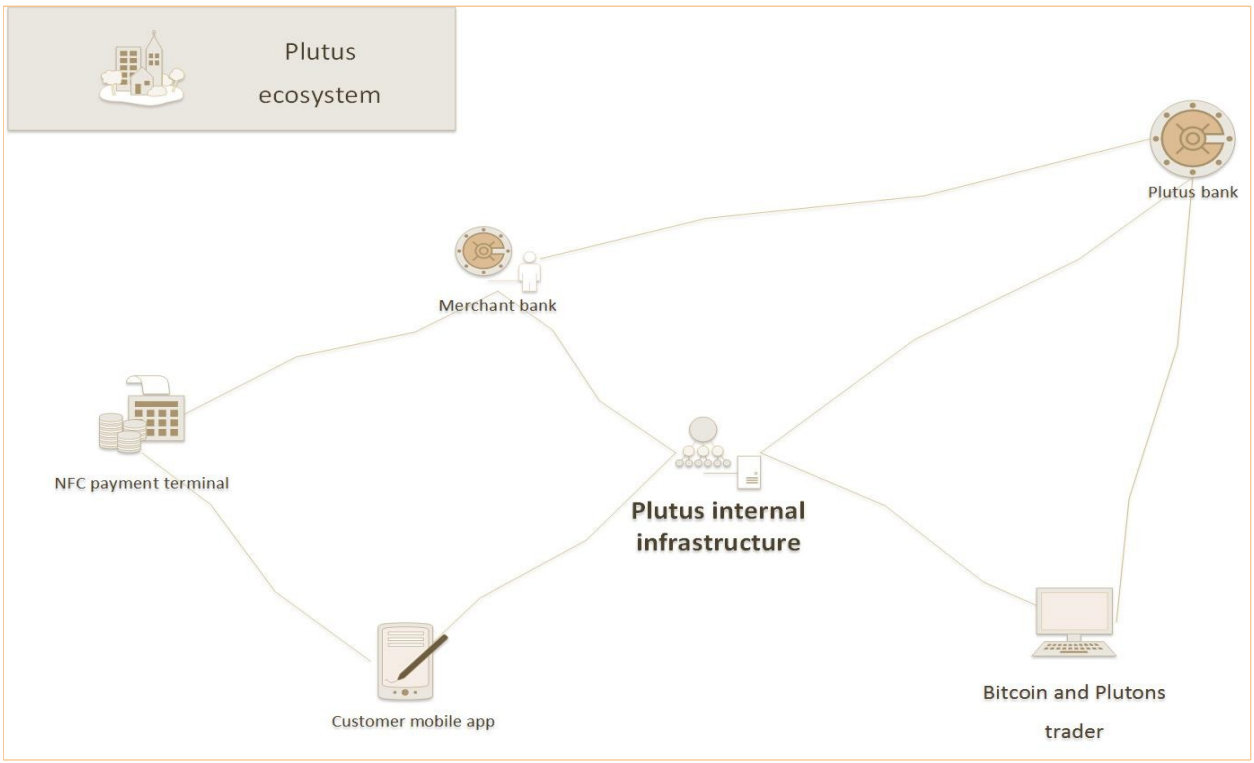

Figure 1: The Plutus Ecosystem

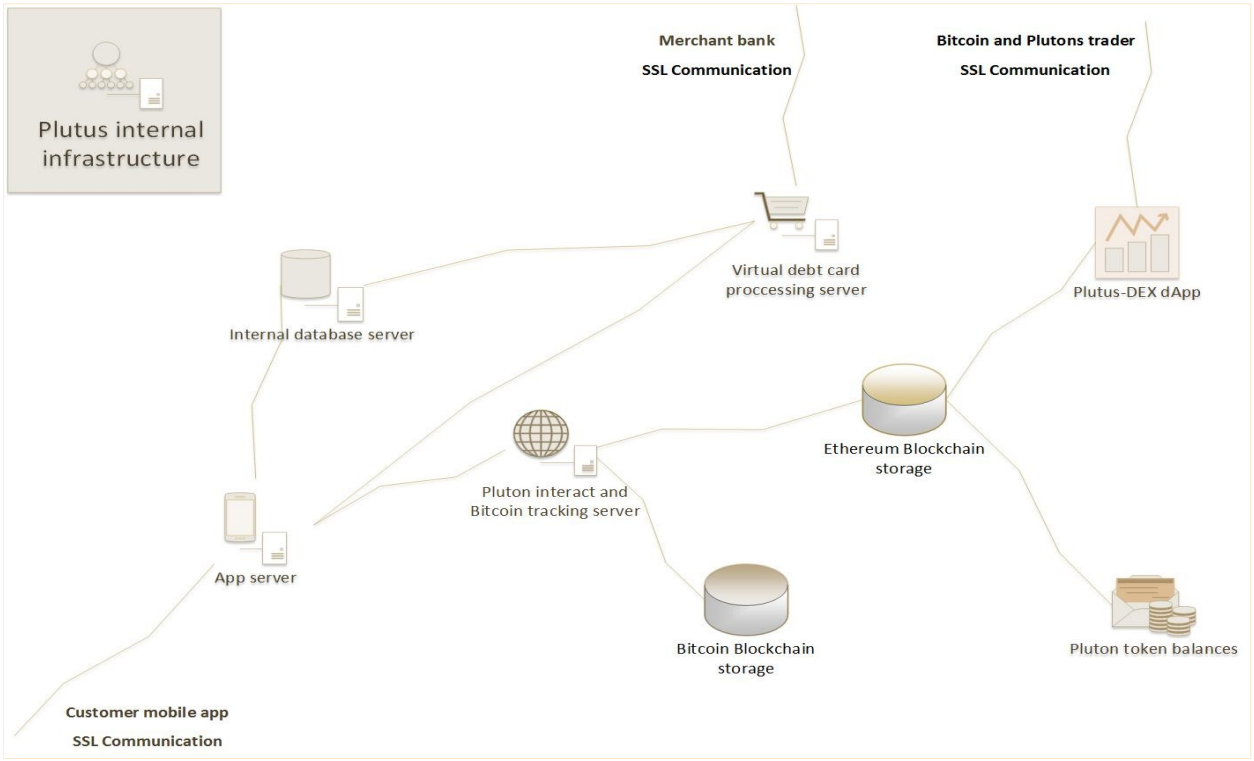

Figure 2: The Plutus Internal Infrastructure

the Plutus app server, which in turn communicates with the other network servers. The Bitcoin tracking server reads transaction data contained in the header of each block broadcast onto the Bitcoin network to confirm when payments have been completed. Plutons are divisible and tradable assets created on the Ethereum network. This ensures that all Plutons, whether they are traded or transacted between users, are safely confirmed, and permanently stored on the Ethereum blockchain.

The PlutusDEX, or DEX, is a dApp (decentralized application) on the Ethereum blockchain which handles Bitcoin and Pluton trading and matches orders. Traders can register at `http://dex.plutus.it` to interact with other users on the decentralized exchange to purchase Bitcoins and Plutons using fiat moneys, i.e. GBP, USD, or EUR. The dApp parses the data from each trader's price and quantity submitted to the exchange. The Bitcoin tracking server monitors the address of each user of the mobile app. As a user deposits Bitcoins onto their mobile app, the amount is instantly matched with the best valued offer from a DEX trader, and the user is sent their rebate reward in the form of Plutons. The DEX trader sends the correct amount of fiat currency to the Plutus Escrow, where it is then relayed to the merchant's bank and completes the transaction cycle, as shown in Figure 3.

1. An app user enters an amount of Bitcoin to deposit. The DEX dApp instantly matches the request with the best price provided by verified traders on the PlutusDEX platform, along with the corresponding Bitcoin and/or Pluton payout address.
    1. A Bitcoin or Pluton deposit request is sent to the DEX dApp running on the Ethereum blockchain via the Plutus internal server.
    2. Offers and bids are matched using the DEX dApp, resulting in a sale of digital tokens for fiat currency at the current market rate. The DEX dApp sends an "event" message to the app user containing the public address of the trader who exchanges the user's Bitcoin for fiat.
2. The DEX dApp receives blockchain transaction verification via the Plutus tracking server, which interacts with both the Bitcoin and Ethereum blockchains. Upon confirmation, the DEX dApp marks the transaction as complete.
    1. A notification is sent to the Plutus Internal Server.
    2. The Plutus internal server (centralized) confirms deposits and transaction details on the Bitcoin blockchain, as well as on Ethereum's blockchain. It then sends the event message to the DEX dApp (decentralized) running on the Ethereum blockchain.
3. Traders must verify their account and identity on the PlutusDEX platform to enable any transfer of funds to the Plutus escrow account. A trader can then enter trade information (create a bid) on the DEX dApp. Traders announce their payout wallet address in advance, in order to receive Bitcoin or Pluton deposits directly from app users.
    1. Traders can use any valid Bitcoin address, and hold their own private keys. Offline wallets and cold storage are recommended.
    2. Deposits of fiat-currency to Plutus escrow is completed via the DEX dApp. Details of all trades and deposits are stored on the Ethereum blockchain.
4. Next, the Plutus internal server receives verifications from the Ethereum and Bitcoin blockchains of the completed transaction stored within the DEX dApp. Funds are immediately deducted from the DEX user's escrow account and then released to the prepaid virtual debit card on the mobile app in the selected local currency.
    1. The Virtual Debit Card (VDC) gateway enables contactless balance creation in GBP, USD, and EUR.
5. The merchant then receives payment authorization via the VDC gateway. Funds in their preferred currency are forwarded to the merchant's bank through the established worldwide debit card banking network.
    1. Finally, a transaction confirmation is sent to the app which triggers an update to the contactless balance for the mobile app user.

2.1 The PlutusDEX Platform

The PlutusDEX platform, illustrated in Figure 4, consists of two main components:

1. The *PlutusDEX dApp* that runs on the Ethereum network.

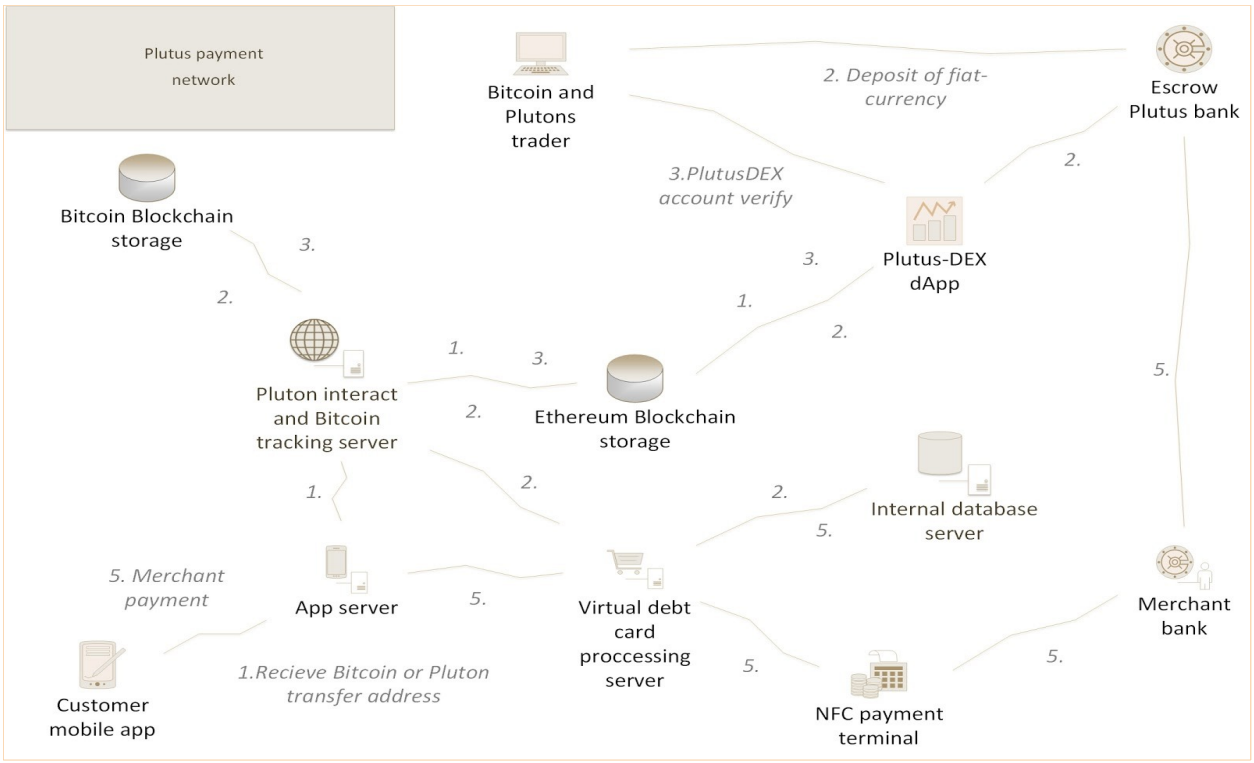

Figure 3: The Plutus Payment Network

2. *Applications* that form a bridge between Ethereum and the traditional payment infrastructure.

The PlutusDEX platform features the utilization of Ethereum dApps to execute trades between app users and traders in a peer-to-peer system. The DEX dApp matches bids for Bitcoin and Plutons. The platform itself supports fiat deposits and offers traders access to purchase Bitcoin directly from app users.

2.2 Plutus Mobile App

The Plutus Mobile App (Figure 5) connects users directly to PlutusDEX traders on the Ethereum network. Using the Plutus internal server, the Bitcoin network can be reached using the native Bitcoin API, which is connected to via the Java API (ethereumj), or alternatively, the Javascript API (web3).

The Plutus Mobile App enables the user to choose among a selection of different fiat currencies. A virtual debit card account can be created in GBP, USD, or EUR, allowing the user to have multiple payment options.

2.2.1 Plutus App Fee Optimization

Bitcoin conversion has a fee of between 1-4% (TBD). The fee is deducted from the users' fiat deposit balance before the money is released to their VDC account on the Plutus Mobile App. There are no other fees for using the app and no fee to deposit Plutons on the app obtained from another user externally. Plutus pays all transaction costs associated with using the Ethereum network (See Section 2.4.2). Merchants pay their normal debit card payment processing fees.

2.3 Plutus Payment Process

The Plutus payment process (Figure 6) consists of two main actions:

1. The Plutus Mobile App initiates a wireless payment to the merchant's NFC-enabled payment terminal through the user's NFC-enabled smartphone.

2. The user's VDC payment authorization is sent to the merchant's payment processor, and once approved, the funds are deposited to the mer-

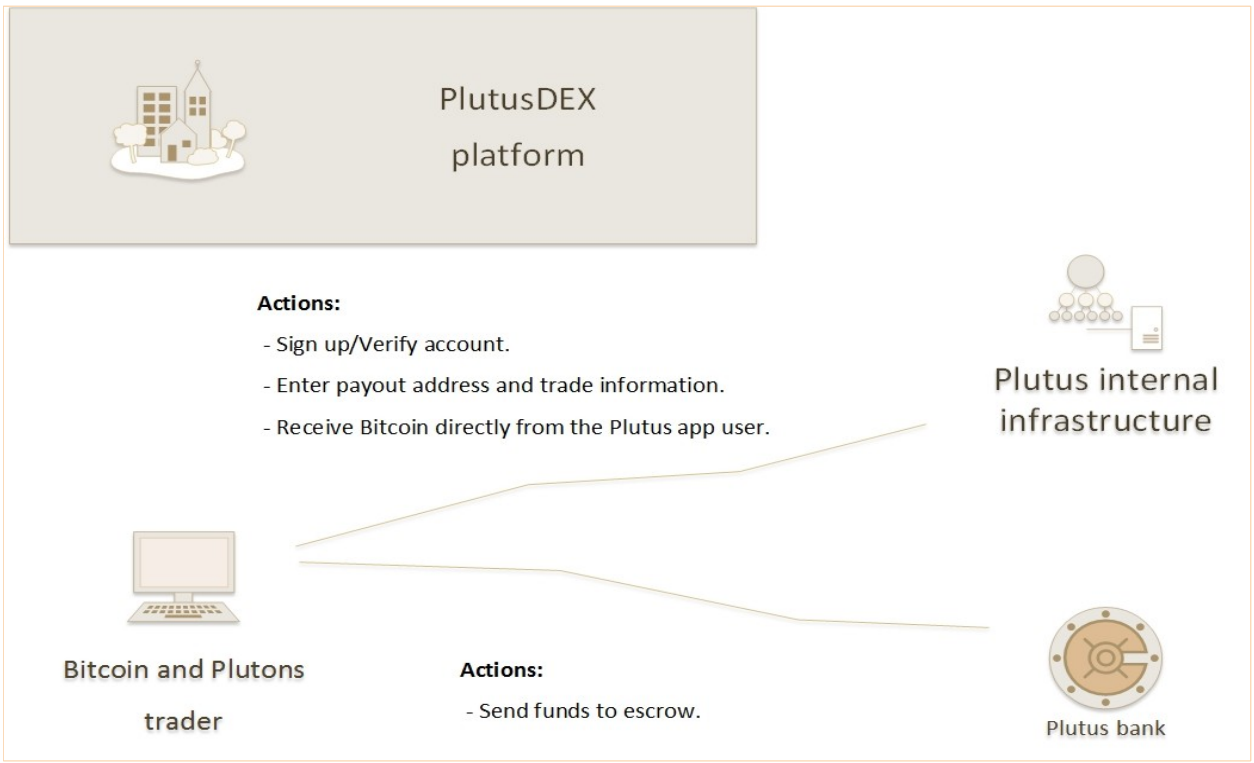

Figure 4: The PlutusDex Platform

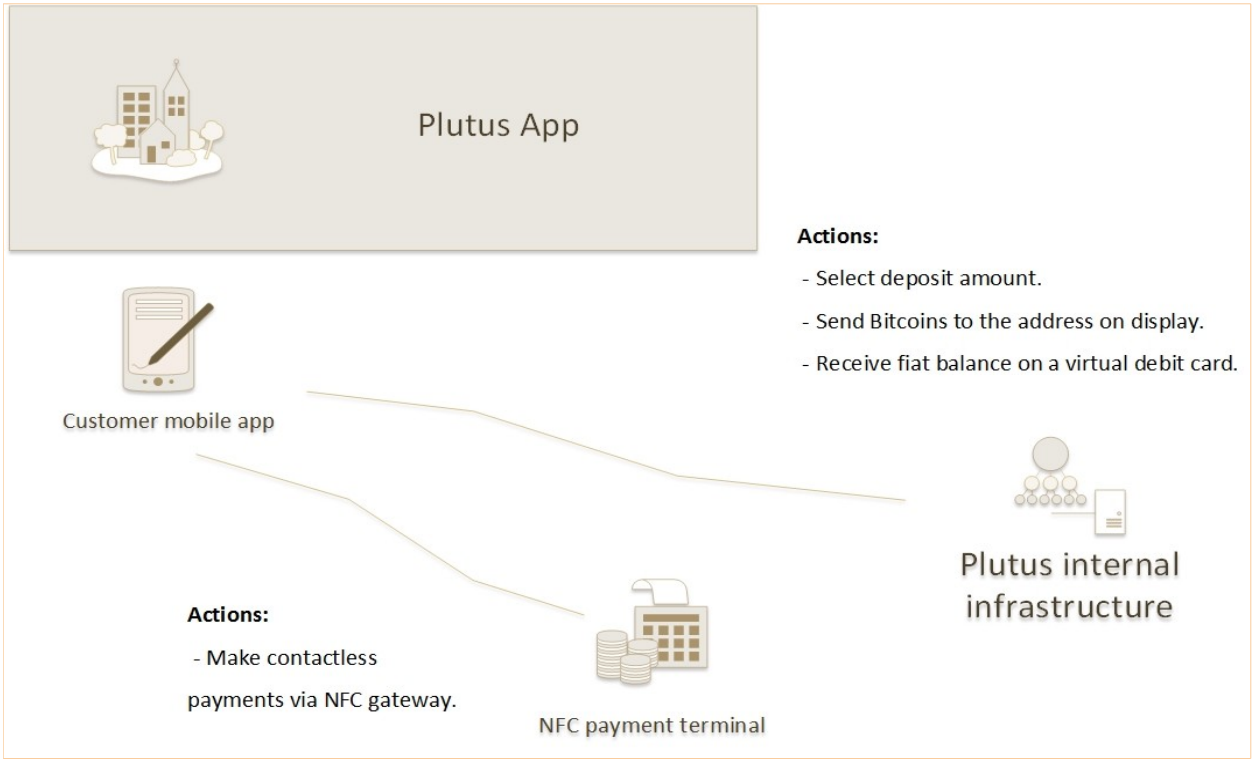

Figure 5: The Plutus App

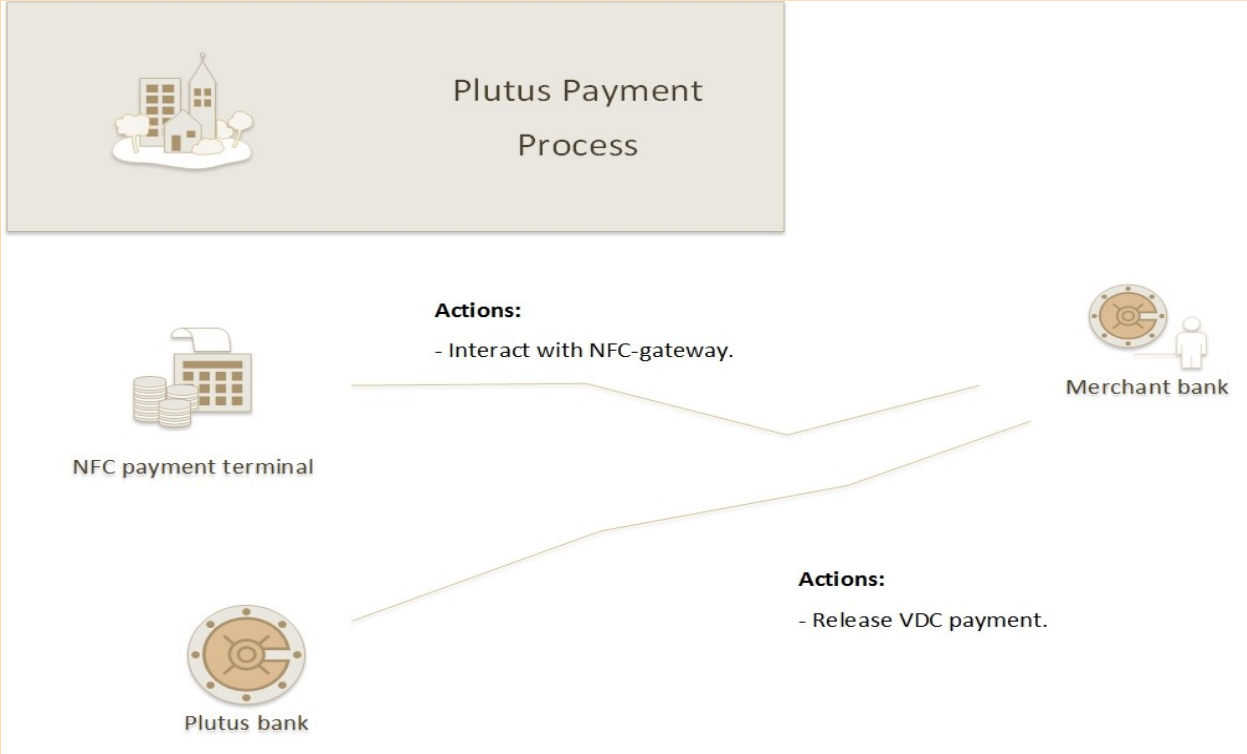

Figure 6: The Plutus Ecosystem Actions

chant's bank account. The user and the merchant, respectively, receive confirmation of a successful transaction.

2.4 Pluton Token Infrastructure

Plutons are the internal digital asset of Plutus and are issued on the Ethereum blockchain. Pluton transactions can be sent and received using the Plutus Mobile App, similarly to Bitcoin. Plutons have the added benefit of zero transaction fees, as well as instant transaction confirmations.

Ownership of Plutons is tied to an Ethereum account. Pluton token source code — running on the production Ethereum network (networkid 1) — acts as a decentralized and distributed ledger of all Pluton transactions and the addressed location of every Pluton. The benefits of using Ethereum's blockchain is its reliability, underwritten by Ethereum's built-in incentives for securing the blockchain. This ensures the continuity, integrity and security of the Pluton ledger.

The Ethereum network supports near-instant confirmations of Pluton transactions. According to the latest data, the average time for a new transaction to be confirmed on the blockchain is approximately 17 seconds. This enables users to convert their digital assets to fiat currency in nearly an instant.

2.4.1 Pluton Rebate System

Plutus Mobile App users are rewarded with a rebate, at a predetermined rate, of Plutons for every Bitcoin-to-fiat exchange they make in order to fill their VDC balance. Plutons can be exchanged for fiat currency that is then instantly credited to the user's contactless balance. There is no rebate reward given for exchanges of Pluton and fiat currencies.

The Pluton Rebate System (Figure 7) is implemented on the Ethereum network and regulated by the DEX. Plutons received as rebate rewards are distributed automatically by the DEX to Plutus Mobile App users.

There will be 20,000,000 total Plutons in existence. As the trading begins for Plutons on the DEX network, the exchange rate, E_P, will fluctuate according to market conditions. Its general equation can be described as the amount of Plutons, P_t, required to

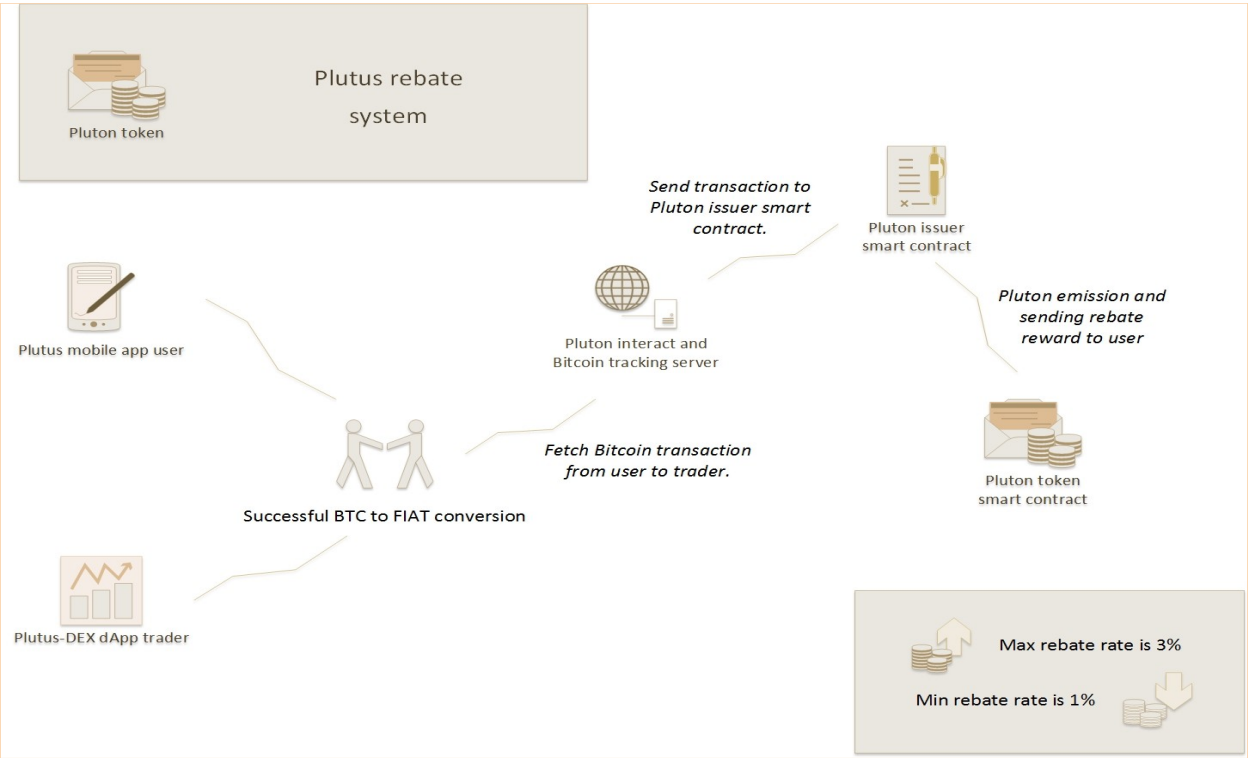

Figure 7: The Plutus Rebate System

trade for one Bitcoin, or

$$E_P = \frac{P_t}{1BTC} \tag{1}$$

Bid orders for Plutons are made via the trading frontend. The PlutusDEX trading API will be open source. It will enable the participation of users on the DEX network once they have been verified on the frontend.

Users can buy Plutons, as well as Bitcoin, using the DEX. Plutons earned via rebates can be transferred on the blockchain and have no restrictions on use with in the payment system. Users can transfer Plutons to other users or trade them for fiat currency, which is sent to the users' VDC balance for in-store purchases. Plutons are implemented as a 'Transferable Fungibles' e.g. sub-currency on Ethereum, using the standard Ethereum API.

Since rebate rewards are only dispersed when converting Bitcoin to fiat money we must utilise the variable exchange rate of, E_{BTC}, Bitcoin to the British Pounds, expressed as

$$E_{BTC} = \frac{1BTC}{T_t GBP} \tag{2}$$

where T_t represents the current amount of British Pounds required to purchase one Bitcoin as dictated by the market.

Let T_i symbolize a single transaction by a single user, worth no more than a maximum value of £30. Multiplying T_i by equation (1) yields the Bitcoin value, B_i, of the given transaction,

$$B_i = E_{BTC} * T_i \tag{3}$$

where $T_i \leq £30$.

The rebate reward rate, R, changes every 24 hours according to the previous day's aggregate Bitcoin transaction volume, $V^{\triangle}$, expressed as

$$V^{\triangle} = \sum_{i=1}^{n} B_i^{\triangle} \tag{4}$$

where the symbol, $\triangle$, in the superscript indicates that it represents data from the previous day. The previous day's aggregate Bitcoin transaction volume is obtained above by summation of each instance of equation (3) on the previous day.

The rebate reward rate is determined by an algorithm (Figure 8), where R is a dependent variable to $V^{\triangle}$ by adapting and modifying the model of a step function to a non-Boolean use. The indicator function of R is defined as the interval expression, $I_{V^{\triangle}}$, with the subscript, $V^{\triangle}$, of equation (4), which acts as the interval parameter function of the next day's rebate reward rate, defined by the expression

$$R := I_{V^{\triangle}}(R) \tag{5}$$

The interval parameter function is defined by the variable values of R, which are dependent on the corresponding range of the previous day's Bitcoin transaction volume, $V^{\triangle}$.

$$I_{V^{\triangle}}(R) := \{R_i, m_i \leq V^{\triangle} \leq M_i \tag{6}$$

The rebate rate, R_i, in the above expression represents the general structure of the parameters that describe every possible value. Each daily rebate rate, R_i, must differentiate from the previous day's rate, $R^{\triangle}$, by $\pm 0.01\%$, while $M_i - m_i = 0.1BTC$ at each step. The maximum rebate rate is set at 3% when the daily volume is 5 BTC or less and 1% when the daily volume is 25 BTC or more. Thus, each daily increase in volume of 0.1 BTC will reduce the rebate rate by 0.01%, and vice-versa.

The PlutusDEX dApp calculates the previous 24hr Bitcoin deposit volume on the network to determine the rebate amount for the following 24hrs on the app. This data is relayed to the Pluton issuer code and the change is affected immediately.

Now that the rebate reward rate, R, has been found above, we can find the amount of Pluton, P_i, for one user's single transaction by multiplying the results of equation (1), equation (3), and the current exchange rate, $R^{\triangle}$, to find

$$P_i = E_P * B_i * R^{\triangle} \tag{7}$$

The rebate reward rate has the delta in its superscript to indicate that it was calculated using the previous day's Bitcoin transaction volume as expressed in equation (5).

Finally, we can calculate the total Pluton dispersed to users for an entire day, P_{day}, by summation of the results obtained from equation (3) and equation (7) and simplifying to obtain the emission equation:

$$P_{day} = R * \sum_{i=1}^{n} (P_i * B_i) \tag{8}$$

2.4.2 Smart Contracts & Functionality

On the Ethereum blockchain, dApps are regulated by their underlying code, commonly called a *smart contract*. Plutus has several types of interacting contract code, each with an important function. Each instance can be called via the internal infrastructure, the Plutus web-application (client side), and/or the Plutus Mobile App. When an instance is called, the result is transmitted, asynchronously, as an Ethereum *event*.

These *events* will handle all Plutus transactions between traders and users; will register new deposits of fiat currency; and will regulate the issuance of new Pluton tokens, earned by users as rebates. Every time a Plutus smart contract is called, a small amount of Ether must be payed as a transaction fee for Ethereum miners. This fee is known as the *Gas Price* and is paid for by Plutus.

Each instance of a Plutus *smart contract* is explained in more detail below. Their interactions are illustrated in Figure 9:

- *Plutus User Contract*: This is created for each user and each trader who register. Users can register through the Plutus Mobile App. Due to Know-Your-Customer (KYC) rules, users must identify themselves using the Plutus central service, or through an external service such as Uport. The user contract itself will contain a limited amount of logic, but it does reference other smart contracts such as PlutusDEX contract and the Pluton token contract.

- *PlutusDEX Contract*: Enables users to exchange Plutons, fiat currency and Bitcoin. Traders can deposit fiat money using the Plutus centralized web-application. After verification by the Plutus internal infrastructure, users can trade by directly interacting with the smart contract through the standard client provided by Plutus, or by using a custom client.

- *Pluton Token Contract*: Determines the Pluton balance of every user on the Pluton network and

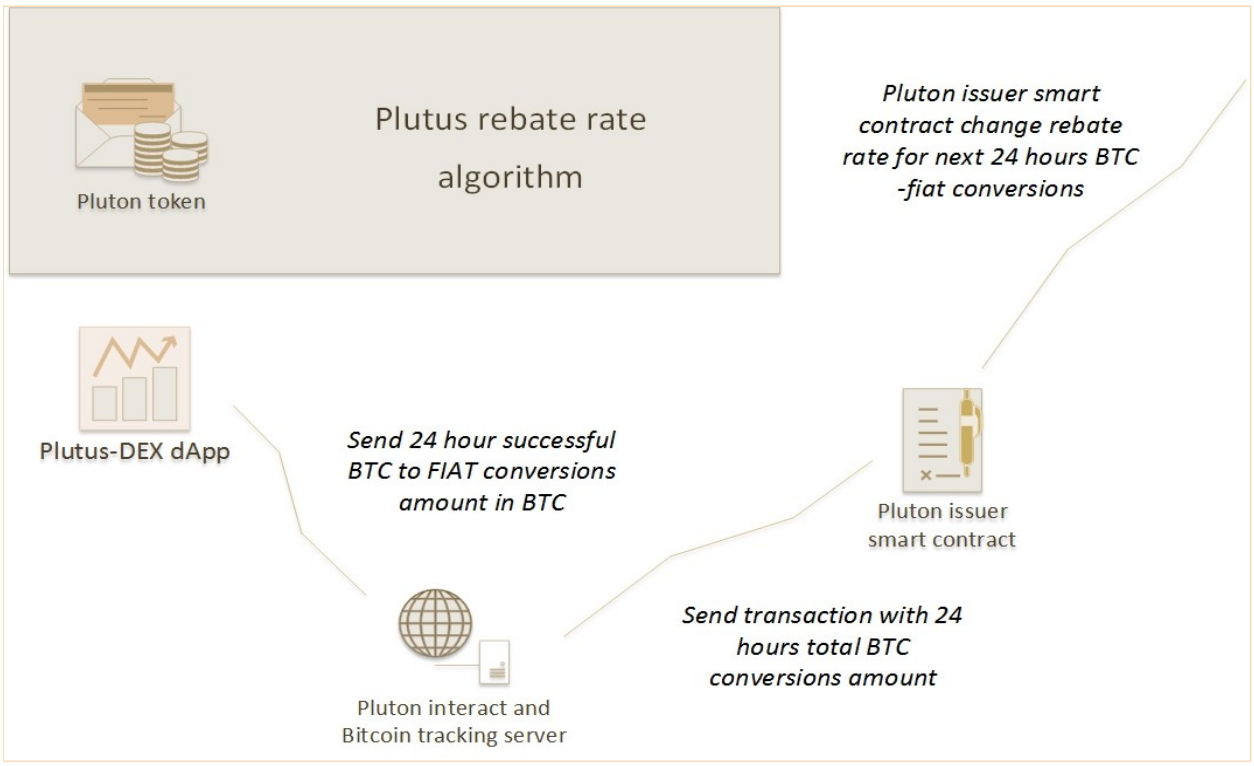

Figure 8: The Plutus Rebate Rate Algorithm

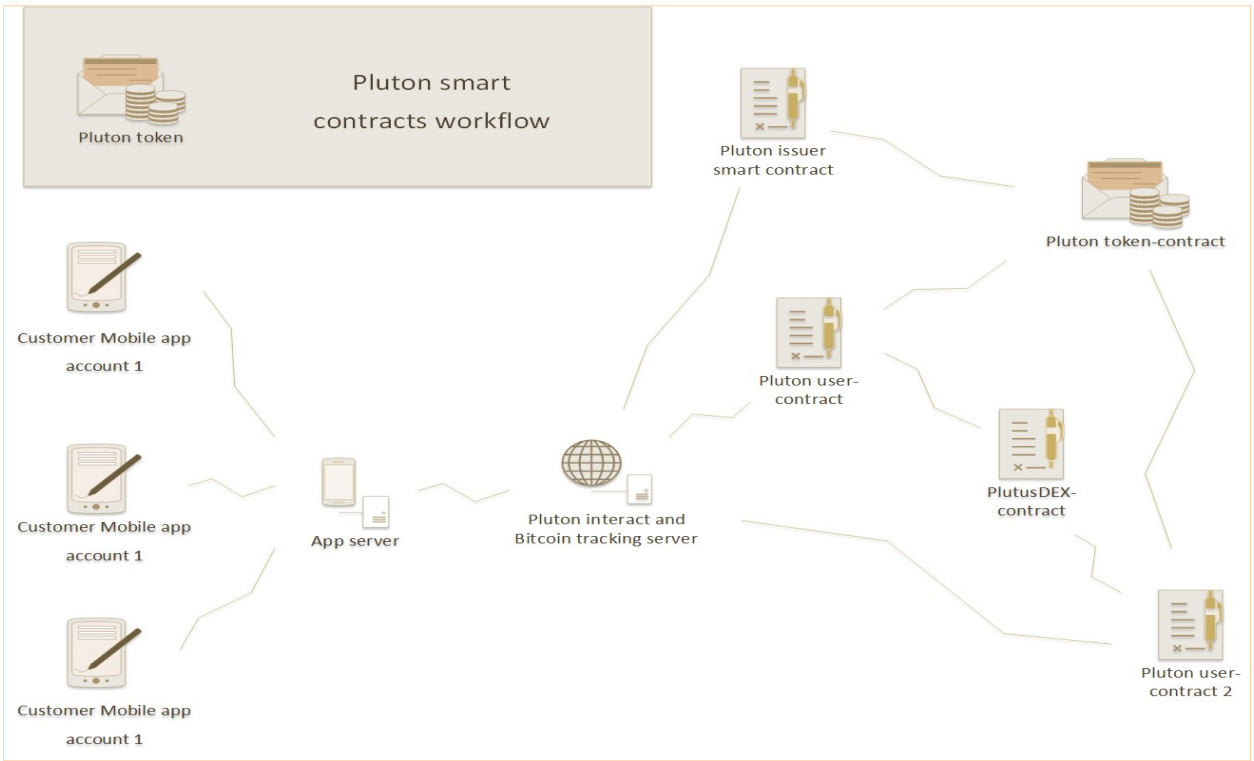

Figure 9: The Pluton Smart Contracts Workflow

uses the standard Ethereum API where applicable. Users can view their balance and create Pluton transactions using a wallet that supports the transferable fungibles standard, through the plutons.sol ABI definition. For example: see Mist Wallet 0.3.5 (Beta 3) release.

- *Plutus Issuer Contract*: Regulates the amount of Plutons issued as rebate rewards for Plutus users. The contract uses the process detailed in Section 2.4.1. Rewards are based on the amount of Bitcoin that a user trades for fiat currency each day. Only Plutus central can issue rebates.
- *Name Registry Contract*: Holds the addresses of all active Plutus smart contracts, and allows other smart contracts to call it to return specific addresses on the Ethereum blockchain. See namereg.sol for example code.

A more detailed overview of Plutus smart contracts and how they interact can be found in Section 4. Plutus smart contracts are being actively developed as open source software viewable on the Plutus Github. Readers are encouraged to comment or supply patches to the source code.

Example of an smart contract source:

```
function Issue(address _issuer, coin _plutonAddr) {
        issuerAddr = _issuer;
        coinAddr = _plutonAddr;
        rebate.baseUnitForRebate = 1000;
        ...
        dayBtcVolume = 0;
        volumeUpdateTimestamp = now;
        pluton = coin(_plutonAddr);
    }

    function updRebateRate(uint _lastDayBtcVolume) ownerCheck returns(uint
plutonRewardRate) {
        if(_lastDayBtcVolume > dayBtcVolume) {
          ...
        }
        return(rebate.plutonRewardRate);
    }
```

Figure 10: Pluton Rebate Code

2.5 Virtual Debit Card Gateway

A DEX trader transfers fiat funds to the Plutus escrow account prior to entering trade information. Only the Plutus virtual debit card gateway application can release the fiat balance to a virtual debit card token. This is a secure token used for authorization, which is sent to the merchant's payment processor via the NFC mobile device. The fiat amount is released to the merchant's bank-account via the debit card payment network, once the trade has been completed.

- VDC gateway connects to the Plutus app.
  - VDC provider's API enables users to generate a single virtual debit card token for each selected currency (GBP, USD & EUR).
  - A Plutus app account only allows one VDC account per currency. Each new deposit will be added to the same VDC account.
- VDC gateway connection to NFC device.
  - Plutus app user initiates a purchase cycle, by contacting the merchant's NFC-enabled POS terminal (contactless card reader).
  - The mobile device's built-in NFC capability is used to send the VDC token-authorization code to the merchant's payment processor or bank.

3 Trust & Security

The app user preloads his VDC using Bitcoin. The request is stored on the Ethereum blockchain, rendering it transparent and decentralized. This request is handled by the DEX, which sends the trader's payout address to the Plutus Mobile App. The app then transfers Bitcoin directly to the payout address provided by the trader.

Since public addresses of traders are published on blockchains, and therefore known to the Plutus platform, the Plutus platform can verify that the amount transferred to the traders' accounts is correct before releasing the fiat balance accordingly. The VDC-provider receives the fiat amount and loads balance to the customer's VDC.

The app is designed for small day to day payments only. It has a deposit limit for different account types and a per transaction limit of £30 in the UK (minimum transaction limit changes according to location). Users will be advised to only deposit what they wish to spend. In case of user error where the deposit amount is more or less than the requested amount, the smart contract will notify Plutus of the anomaly and fund the user's VDC account accordingly.

Note: Traders receiving deposits have verified identities using KYC/AML procedures and have fiat funds secured in escrow. There is a minimum balance limit for traders on the DEX to protect against anomalies linking to incorrect deposit amounts.

Solidity
Bitcoind
Web3 API

4 Development Technology & Smart Contract Stack

Anyone with a contract address will be able to access data. However, only people with access to certain Ethereum accounts will be able to modify or enter data.

Table 1: Plutus Contracts

Contracts	Contract interface	Storage	Events
Trader contract		Active traders	TraderRegistered
DEX smart contract	Dex interface	Deposited Bitcoin, deposited fiat currency	BitcoinDeposit, FiatDeposit. BitcoinFiatTrade RebateReceived other events
Pluton Token	Standardized currency api	Token ownership	CoinSent
Name registry for contracts	Standardized name registry	Registry of contract names and addresses	Changed

Table 1 Links:
Standardized Currency API
Standardized Name Registry

Table 2: Plutus Accounts

Account Types/Roles	Number of Accounts	Access
Plutus Board	1	Name registry for updating Plutus contracts
Plutus Virtual Debit Card Gateway	1 or equal to # nodes running VDC gateway	Tracking fiat currency transfer, matching with escrow bank transactions
Pluton Distributor	1 or equal # Issuer smart contract	Access to contracts for Pluton emission.
Trader	For each trader that will subscribe/1 for trading platform	
User	For each app user/1 for user platform	

Table 3: Plutus Infrastructure

Table 4: Blockchain Transactions

Table 5: Implementation

Table 5 Links:
Windows Phone
Go-Ethereum
Web3.js

Glossary

Bitcoin a digital peer to peer currency.

blockchain a permissionless distributed database that maintains a continuously growing list of data records secured from any tampering or revision.

escrow Bank account to secure fiat deposit from the network.

Ethereum a next-generation application platform based on blockchain technology.

fiat currency National currency issued by a central governing organization such as the European Bank or the Bank of England or the US Federal Reserve.

Near Field Communication (NFC) Allows a mobile phone to communicate with a payment terminal.

peer-to-peer (P2P) A network in which each computer can act as a server for the others, allowing shared access to data without the need for a central server.

Plutons Rewarded to users when depositing Bitcoin. Built for instant confirmations and issued on the Ethereum blockchain as a digital token.

Plutus Internal Infrastructure Central software hosted on servers to provide the platform for traders. It acts as a bridge between the blockchain and the VDC as well as the mobile application.

Plutus Mobile Application Allows conversion of Bitcoin and Plutons to Fiat currency balance on a virtual debit card token to pay merchants.

PlutusDEX Decentralized Exchange logic running as smart contracts on the Ethereum network.

smart contract A computer protocol that facilitates, verifies, or enforces the negotiation or performance of an agreement between multiple parties.

trader Plutus app user who buys Bitcoin in exchange for for fiat currency.

user a consumer with an NFC-enabled mobile device with the Plutus Mobile App installed on their device.

Virtual Debit Card (VDC) A debit card that is issued and usable on a digital device without a corresponding plastic card.