Теневой банк (миксер)
DApp 86

Платежные системы на основе блокчейна часто имеют проблемы с анонимностью. Это связано с тем, что вся информация сохраняется в блокчейне в открытом виде и можно проследить все транзакции от одного счета до другого.
Мы предлагаем два варианта решения этой проблемы:

1) Использовать миксер денег (когда суммы с разных счетов перемешиваются с друг другом через единый счет смарт-контракта)
2) Использовать зашифрованные транзакций, так чтобы в блокчейне не хранилась информация в открытом виде

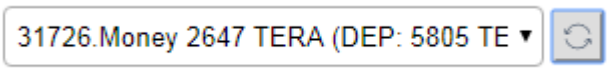
Дапп работает по принципу банка. Вы можете хранить там деньги (без ограничения срока), можете выполнять произвольное количество выводов, а также совершать внутрибанковские переводы (с одного депозита на другой).

Депозиты

Вы открываете депозит, номер которого совпадает с номером счета в вашем кошельке. Открытие депозита происходит путем отправки суммы денег. Дапп имеет ограничение на минимально пополняемую сумму (в тестовой базе это 50 Тера), она отображается на закладке Депозит и видна в момент перевода.

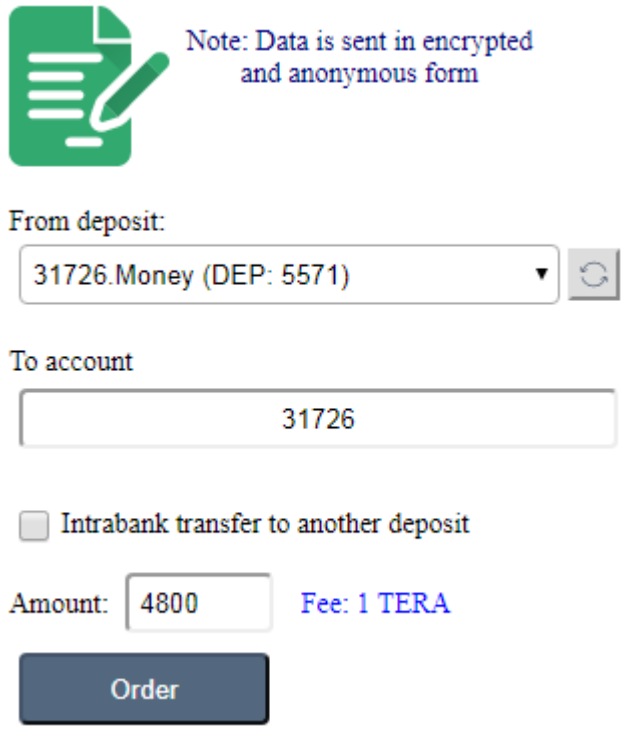
В любой момент можно пополнить счет депозит, просто отправив еще монеты на тот же номер депозита.
Узнать остаток депозита можно нажав кнопку Обновить рядом с номером депозита.

После чего программа проанализирует блокчейн и найдет последний известный баланс по этому счету. Баланс не хранится в открытом виде, он виден только для владельца счета (зашифрован приватным ключом кошелька).
Если баланс найден, то информация по депозиту отобразится в виде доп строки “(DEP: XXXX)”:



Переводы

Для того чтобы вывести деньги на другой счет служит закладка Ордера. В нем вы указываете номер депозита, счет на который хотите перевести деньги и сумму. За перевод берется комиссия. Информация о взимаемой комиссии видна в момент совершения перевода.



Команда отправки ордера совершается анонимно, в ней нет открытой привязки к номеру счета, а вся необходимая для совершения операции информация зашифрована (прочитать может только банк).

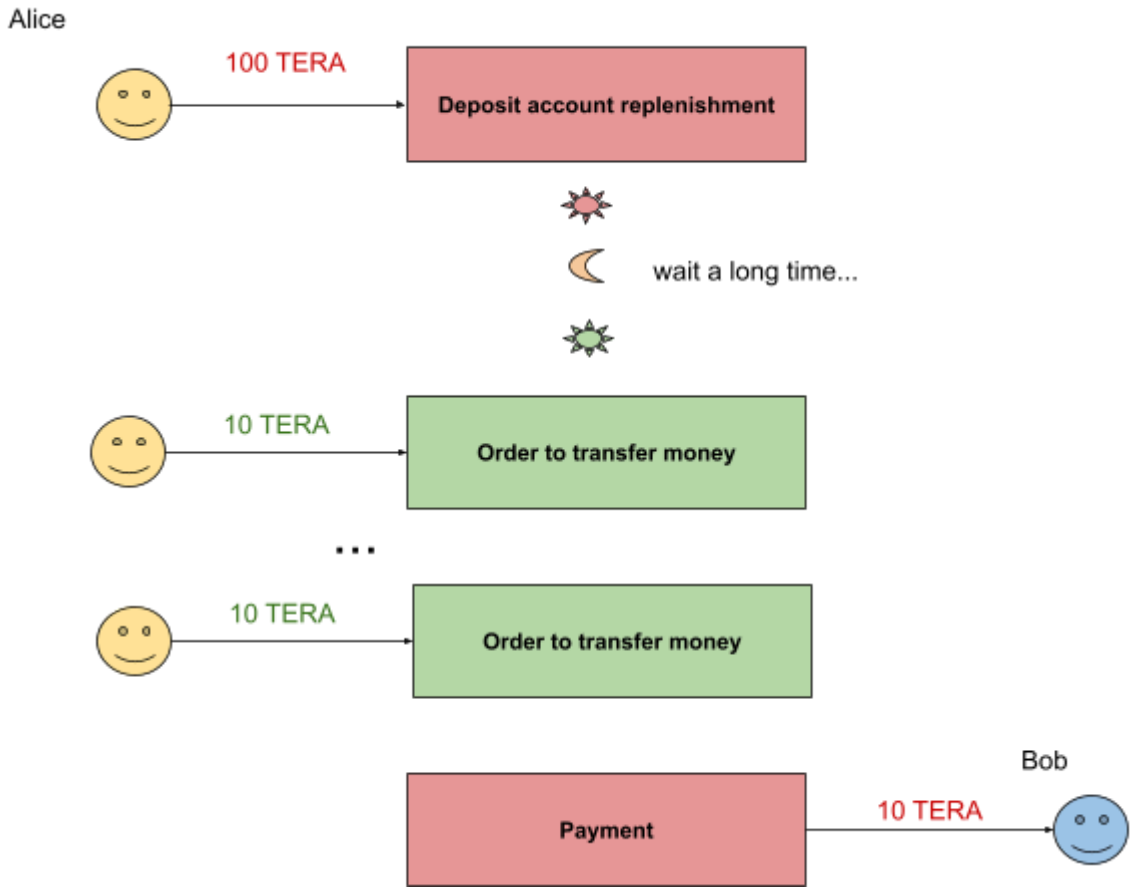
Помимо указания стандартного счета, можно поставить галочку “Перевод на другой депозит”. В этом случае перевод совершится внутри банка (смарт-контракта), а так как информация о переводах зашифрована, то в открытом доступе ничего не будет видно. Получатель платежа может убедиться что платеж совершен зайдя в дапп на закладку Ордера и нажать на кнопку обновить рядом со счетом. При этом ему не нужно совсем привязывать смарт-контракт к счету - привязка нужна только в момент пополнения депозита, в дальнейшем она не нужна и ее можно в любой момент убрать, а потом если нужно - заново поставить.

Банк (владелец) смарт-контракта вправе задавать:
-Признак, что банк открыт на прием депозитов
-Минимальную сумму пополнения депозита
-Размер комиссии за каждый ордер перевода

Рекомендации для повышения анонимности переводов:

1. Проверьте что на счету банка уже есть деньги - в этом случае ваши деньги будут смешаны с уже существующим остатком. Убедитесь что сумма в банке больше чем та сумма которую вы хотите вывести. Чем выше разница, тем ниже вероятность связать платежи с вами.
   Информация об общих остатках банка находится на вкладке Депозит:

2. После перевода убедитесь что прошло достаточное количество времени, чтобы нельзя было связать ввод депозита с выводом денег. Команда указания с какого депозита на какой переводить является анонимной, но ввод денег и вывод денег является открытой операцией, поэтому рекомендуется чтобы эти две операции были разнесены во времени. А еще лучше чтобы между вашим вводом и выводом были проведены операции других пользователей.
3. Старайтесь чтобы сумма депозита не совпадала с суммой платежа (вывода денег). Вы можете пополнить депозит на большую чем нужно сумму денег. Остаток будет лежать и ждать следующей команды платежа.

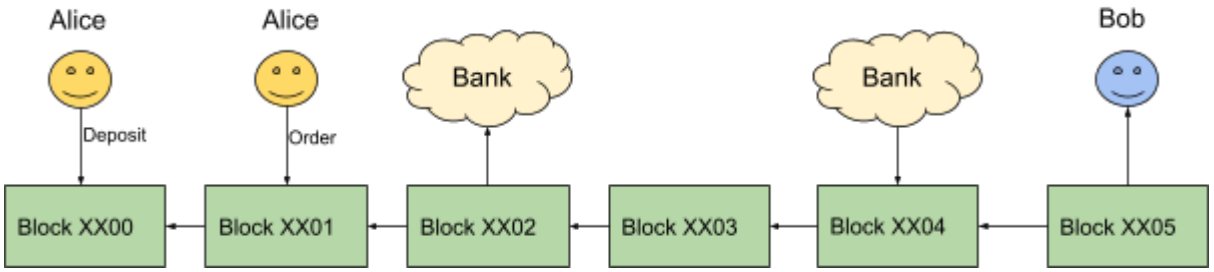


4. Чаще используйте внутридепозитные переводы. В этом случае обеспечивается максимальная анонимность, т.к. все операции зашифрованы. Если вы получили платеж в виде перевода на ваш счет внутри банка, то вы можете не выводить деньги на свой счет в кошелек, а оставить для оплаты другим контрагентам в виде внутридепозитных переводов. В этом случае будет невозможно отследить ваши платежи на основе открытой информации блокчейна
5. Процессинг выполняется централизовано, поэтому мы рекомендуем пользоваться этим даппом, только если вы полностью доверяете этому оператору (владельцу смарт-контракта).

Рекомендации для банка:
-Автоматический процессинг платежей выполняется централизовано на стороне оператора банка. Не нужно писать бэкэнд-код, который будет выполняться на сервере, просто оставьте открытую форму dapp и запустите включите автозапуск (галочка Autorun).
-Используйте максимально безопасную от взлома платформу в которой закрыт root доступ на уровне операционной системы, например устройствах на базе iOS.

Архитектура

Процессинговый модуль банка - модуль который решает на какие счета перевести деньги не взаимодействует напрямую с клиентом. Они общаются только через блокчейн, который является своеобразной шиной данных. Клиент и банк могут находиться в произвольных частях мира и их местонахождение неизвестно друг другу. Клиент отправляет управляющие команды в блокчейне (такие как пополнение/перевод/списание депозита). Оператор банка (в виде клиентской части дапп) читает эти команды в порядке их очередности и по мере своей возможности. В случае валидности таких команд - он отправляет в блокчейн транзакции перевода денег и изменение баланса депозита.



MAIN-NET: https://terawallet.org/dapp/86
TEST-NET: http://dappsgate.com:88/dapp/63
Получение тестовых монет: http://dappsgate.com:88/dapp/16