Kirobo - White Paper (brief)

'Undo' Button for Transactions (Available for Bitcoin)

Abstract

Kirobo is an Israeli startup with a single mission: to create a logic layer that sits on top of each individual blockchain and protects users from human error. Our ultimate goal is to make blockchain as simple and secure as online banking.

With support from the Israel Innovation Authority, we have already created logic layers over Bitcoin networks. These days, we are in a continuous process of rolling out advanced services and solutions on top of these layers.

The Problem:

Cryptocurrency transfer is a risky and stressful task
People are prone to make mistakes – but such mistakes cannot be tolerated in cryptocurrency transfers where a single misplaced digit of the transfer value, or a wrong address, can wipe out large amounts of money permanently.

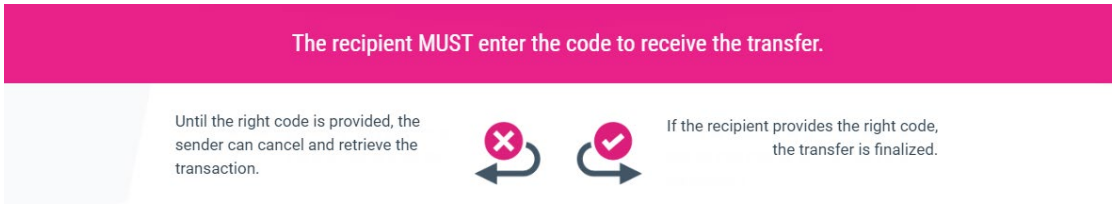
Addresses can also be deliberately altered by third-party attackers, compromising the security of the funds.

Kirobo's Solution

Kirobo adds a new layer of protection to currency transfers.

This layer protects users from all of the above-mentioned scenarios, and works on two levels:

1. A transaction code that must be entered by the recipient in order to receive the transfer
2. Retrieval capability that allows a sender to retrieve the funds at any time, **as long as the right code hasn't been provided by the recipient**



V-4.1
8/2020

Archived copy · cryp2nova.com

A Practical Example

Users can connect to the Kirobo system through their regular wallet (Ledger, Trezor), after which they can create Retrievable (Undo) Transactions

The process on the part of the sender

1. The sender enters the system through safer.kirobo.me
2. The sender clicks on "Send BTC".
3. The sender accesses his Wallet by clicking the Connect button.
4. After the login process, the system scans the customer's accounts
5. The sender selects the desired account
6. The sender performs a standard transaction, except for the fact that he creates a **passcode** and can add a message to the recipient (for example "for invoice 1222")
7. The sender signs the transaction
8. The balance in the sender's account is updated
9. The sender passes the passcode to the recipient

The process on the part of the recipient

1. The recipient enters the system through safer.kirobo.me
2. The recipient clicks on "Collect BTC".
3. The recipient enters **his own address** (the address where he wants to receive the money)
4. The recipient completes the transaction by entering the correct passcode
5. The balance in the recipient account is updated

UNDO for a specific transaction by the sender

1. The sender enters the system through safer.kirobo.me
2. The sender clicks on "Manage My Transactions".
3. The sender accesses his Wallet by clicking the Connect button.
4. After the login process, the system scans the customer's Transactions
5. The sender selects the desired Transaction By checking a check box
6. The sender signs the Retrievable (Undo) Transactions
7. The balance in the sender's account is updated

Clarification

The sender cannot perform a Retrievable (Undo) Transaction if the recipient has already entered the correct passcode.
After a Retrievable (Undo) Transaction is performed, the recipient will no longer see the transaction.

Archived copy · cryp2nova.com

The market

Below is the **daily** number of transactions as of July 2020

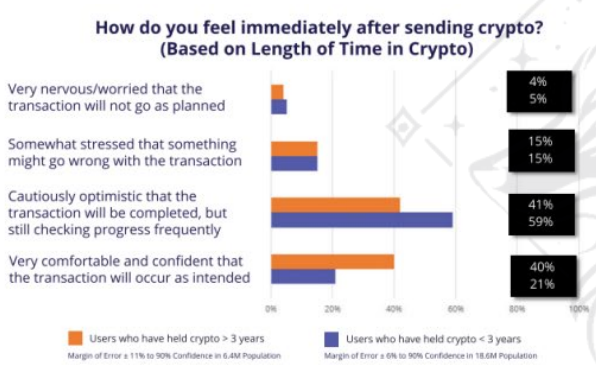
BTC	ETH	USDT(ETH)
340,000	1,143,700	222,000

This means that the Number of Annual Transactions is over **600 million transactions**

How people feel when they send crypto

[1]Below is data based on a survey conducted by FIO protocol

"60-79% of users fear sending money, to some extent "



"57% of users lost or nearly lost money as a result of a mistake



Technical Explanation

- [2]Although reversible transactions in blockchain applications would be desirable, such reversible transactions should not compromise the integrity of data to be stored on a blockchain.

To this end, the disclosed embodiments provide techniques which allow for reversing transactions that will be recorded on a blockchain. Moreover, the disclosed embodiments do not require tampering with the blockchain and, therefore, do not interfere with the inherently secure nature of blockchain transactions. Further, the disclosed embodiments do not require additional transactions to “reverse” the original transaction by returning the transferred assets.

- The various disclosed embodiments include techniques for creating reversible blockchain transactions. In an embodiment, a request to initiate a transaction is received from a first party to a transaction via a first user device of the first party. The transaction includes a transfer of a digital asset such as, but not limited to, funds, keys or other data granting

[1] https://fioprotocol.io/wp-content/themes/fio/build/files/blockchain-usability-report-2019.pdf

[2] PPT 6x/xx5,4xx

Archived copy · cryp2nova.com

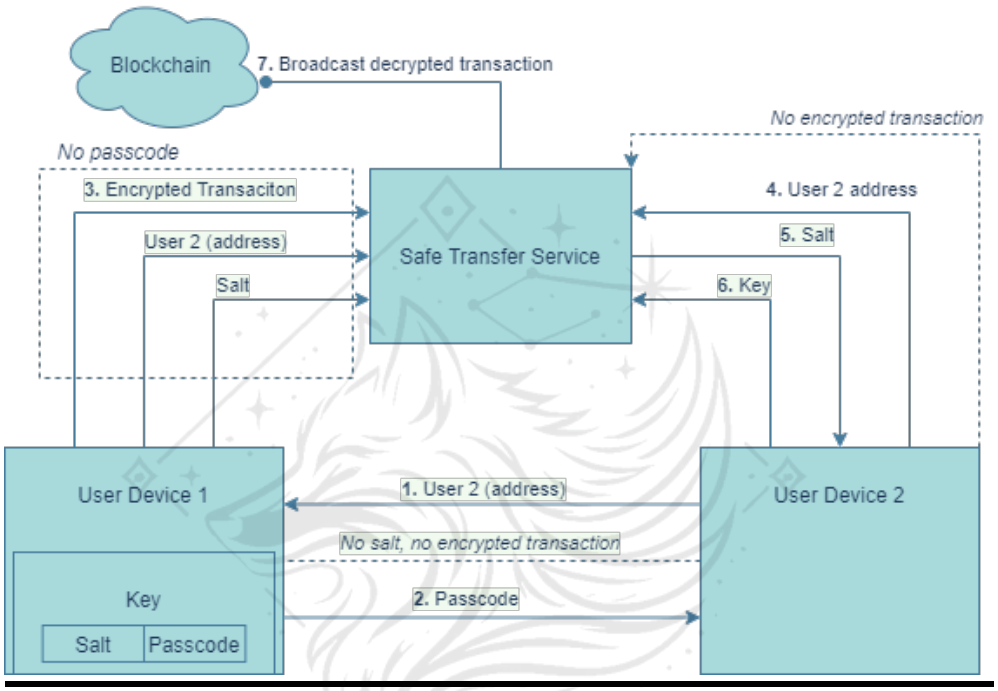
permission to use or control one or more systems, one or more data objects, one or more other digital items which represent ownership of real-world objects, and the like. The request includes data for the transaction signed by the first user device. Transaction data is created based on the signed data, and a hidden address is designated for the transaction. The hidden address is an address on the blockchain which is internal to the first device but hidden to an application which participates in transactions to be recorded on blockchain, i.e., an address which is not known to that application and therefore cannot be accessed by that application.

- In an embodiment, the address is a hidden address with an address including one or more nonstandard parameters such that a blockchain-utilizing application installed on the transferring user device does not recognize the hidden address.
- In a further embodiment, the address includes a change parameter. The change parameter is a value indicating the relative visibility of the digital asset to the first user device. Some existing solutions utilize a value in the address indicating whether the address is visible or not to a program that utilizes a blockchain to record transactions. Such a program may be, for example, a cryptocurrency wallet. Thus, the address including this hidden change value is a hidden address that points to a location which is inaccessible to the blockchain-utilizing program but can be accessed by the first user device upon reversal of the transaction.
- By utilizing an address which is not known to the relevant application installed on the first user device, that application will not recognize possession of the transferred asset. Consequently, the first party cannot use or otherwise access the asset. However, the transferred asset may still be accessed upon request for reversal of the first party using the hidden address. Thus, if a transaction is reversed, use or ownership of the transferred assets may be returned to the first party without requiring altering the blockchain on which the transfer was recorded. As a result, the transaction can be reversed without disrupting the integrity of the data stored on the blockchain or requiring additional transactions to return the transferred assets.
- In an embodiment, a key used for decrypting the encrypted signed transaction data is received from a second user device operated by a second party. The key is sent by the first user device to the second user device. The received key is used to decode the signed data received from the first user device. When the signed data has been decoded, it is re-encrypted and uploaded to a blockchain.
- By using a key sent from the first user device to the second user device, the transaction is secured. More specifically, even if the signed transaction data is sent to the wrong system, the receiving system will not be able to decrypt the signed transaction data and, therefore, will not be able to send the decrypted data for recording on the blockchain.
- The disclosed embodiments allow for reversing transactions without introducing potential issues related to the double spending problem, i.e., a problem which occurs when a digital asset is “transferred” twice. More specifically, the blockchain-utilizing program does not “see” the digital asset stored at the hidden address. For example, when the program is a wallet program, the wallet program will recognize that a certain sum of cryptocurrency has been transferred and will therefore reduce the amount of cryptocurrency available to the user of the wallet program. However, because the transaction data is still stored on the same user device, the cryptocurrency can be refunded without risking spending that sum twice. According to various disclosed embodiments, transactions may be reversed until the transaction data is successfully uploaded to the blockchain.
- Additionally, the disclosed embodiments do not require use of a particular application installed on the user device. In other words, the disclosed embodiments do not require installing a reversible transaction agent on the user devices. More specifically, by utilizing a nonstandard address as described herein, the reversibility of the transaction may be

Archived copy · cryp2nova.com

achieved without reconfiguring the user device. This provides additional convenience and security. More specifically, applications installed on the transferring user device are not required to attempt to tamper with the blockchain or to modify the data on the transferring user device, thereby ensuring the integrity of the data.

System Drawing



Clarification

As can be understood from the explanation and seen in the drawing:

1. The system is trust-minimized and **secure by design** (No single point of failure)
2. At no point does the sender lose ownership of his funds (Until the moment the recipient types in the correct code)
3. The funds are not controlled by Kirobo at any stage
4. The user can return the funds from the "safe address" to his regular address, even without the help of Kirobo (Using our open source CLI tool, which we have released and which can be obtained at the following link)
5. Even if the system is hacked, the worst thing that can be done is to complete the original transaction that the sender intended to perform (This means that the system adds security to the transaction, and does not compromise the original security of the blockchain)

Archived copy · cryp2nova.com

System Integration

Beyond the use of private customers, the system is intended for integration with B2B
B2B customers sign an integration agreement that includes a monthly payment model (SAAS) or a revenue sharing model
There is no obligation to use a KIRO Token to perform integration
However, the use of the KIRO Token can significantly reduce the monthly payment costs of these companies
Library documentation is located here.

Payment for service

The service is offered free of charge for any transaction under $1,000

The commission on a transaction in excess of $1,000 is calculated according to the following formula:

$$\text{The commission} = \frac{\sqrt{\text{Transaction amount}}}{10}$$

In other words, the commission for sending $10,000 is $10, while the commission for $100,000 is $31.60, while the commission for $1 million is $100.

Important clarification - the commission may vary from time to time at the discretion of the company

Commission is paid in the transferred currency (For example if the user sent BTC, the commission is charged in BTC)

Kirobo Utility Token (KIRO)

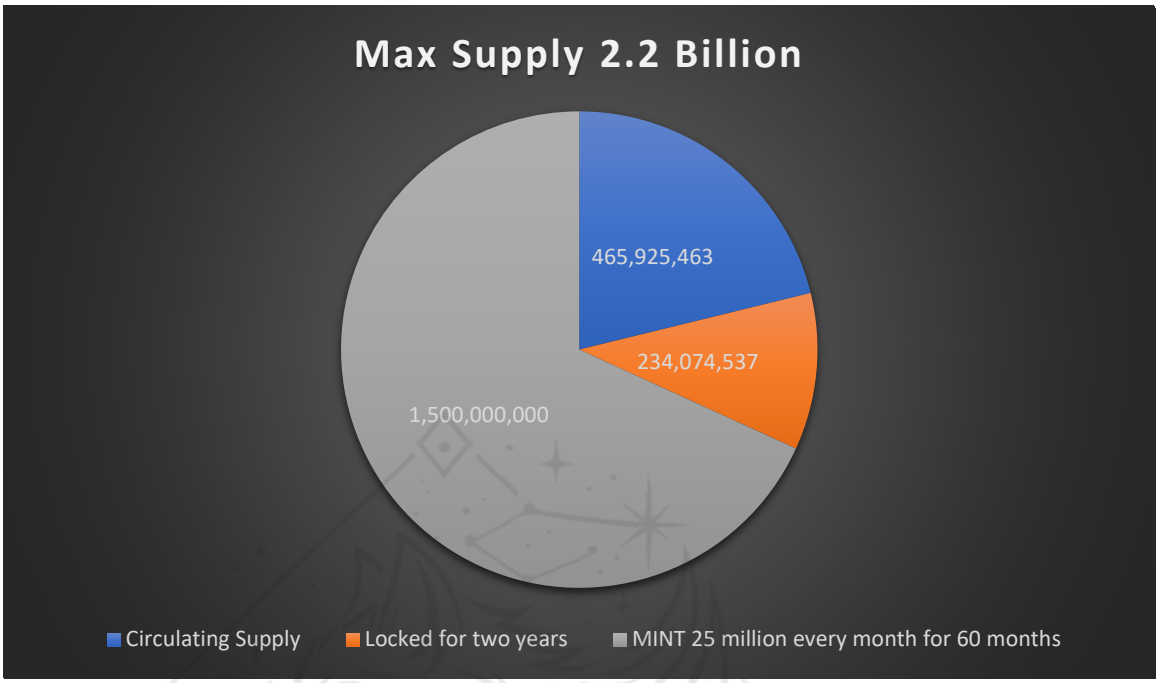
The token is used to reduce network fees by opening a payment channel between the user and the pool contract allowing aggregation of payment by offline transactions.

Token Use

The user will be able to purchase a token through the system (or through an external source such as an Exchange)
If the token is purchased through the system, it is held in a smart contract (pool) which is intended for the aggregation of payments. If the token is purchased through an external source, it must be sent to the pool smart contract to be used for payment of safe transfer fees.
When performing a transaction: If the user owns KIRO and KIRO is held in the designated smart contract, the system recognizes the KIRO and associates it with the wallet that performs the transaction, and therefore does not charge a fee in the transferred currency
For each transaction, the user needs 100 KIRO **regardless of the transaction amount**
That is, if the amount transferred is $1M USD or $5M USD, the KIRO fee per transaction is the same, i.e. 100 KIRO

Archived copy · cryp2nova.com

KIRO (KIROBO) Token



1. KIRO Circulating Supply is **465,925,463** (465 Million).
2. 234,074,537 is locked
3. Total KIRO reserved for sale to Kirobo applications users is **1,500,000,000** (1.5 Billion)
4. KIRO Max Supply is **2,200,000,000** (2.2 Billion)
5. KIRO Token will reach Max Supply in 60 months (five years). Every month 25 million KIROs will be minted (Total 1.5 Billion)
6. **The Company will allow a daily purchase of $300 in KIRO (out of the 1.5 billion reserve)** on the **Company's website**, limited per address.
7. The Company may change the price of KIRO tokens which are sold on the Company's website at its sole discretion
8. The Company may change the daily limit at its sole discretion
9. The Company reserves the right to sell/grant KIRO tokens out of the company reserves beyond the daily limit to partners, large customers, interested parties and ecosystem participants (e.g. staking rewards)
10. The Company does not perform KYC within the daily purchasing limit. However, the company may stop selling to a certain address which is suspected to be an address which is acting in violation of the law and whose source of funds is not clear.

American or Israeli customers are not allowed to purchase the company's Utility

TOKEN, **but they are allowed to use the service** through payment via the transferred currency (for example BTC).

Archived copy · cryp2nova.com

Important Clarification

11. The amount of KIRO required for a transaction can vary according to the company's decision.
12. The amount required for a transaction will never exceed 100 KIRO (this amount may decrease)
13. The option to charge a fee in the currency transferred regardless of the KIRO **will always be maintained**
14. **The company reserves the right to incorporate the token in future products**

Important links

https://kirobo.io - Company website

https://safer.kirobo.me/welcome - Kirobo Safe Transfer deployed on the Bitcoin **mainnet**

https://testsafer.kirobo.me/welcome - Kirobo Safe Transfer deployed on the Bitcoin **testnet**

https://kirobo.io/support/ - Knowledge Base

https://kirobo.io/support/article-categories/video-tutorial/ - Video-Tutorial

https://kirobo.io/support/article-categories/faq/ -FAQ

https://kirobo.io/support/knowledge-base/audit-report/ -Audit Report

https://www.coindesk.com/blockchain-startup-israel-prevent-loss-cryptocurrency-transactions-human-error - Press coverage

Link to 130 articles written about the company's technology (these are not technical articles).
Telegram Channel

Archived copy · cryp2nova.com