White paper - Kirobo

Introduction

Kirobo develops decentralized applications that bring a layer of safety to all of the most popular and lucrative activities in the cryptocurrency ecosystem. Entirely non-custodial, these tools are all provided from a single, consolidated platform called the Liquid Vault. These services can also be used by other businesses via our API.

The Liquid Vault on-chain crypto wallet and management platform provides:

- **Safe Transfer –** enabling password-protected, retrievable crypto transactions
- **Backup –** wallet replacement mechanism preventing loss of asset access
- **Inheritance -** automatic allocation to multiple recipients following inactivity
- **P2P Safe Swap –** direct peer-to-peer token swap service

Future integrations in the roadmap include:

- **Business platform -** API enables other projects to build businesses with our tools
- **Arbitrage -** automatic trades according to price triggers
- **Bridgeless cross-chain connectivity** - enabling access to multiple blockchains via a single interface
- **Mobile app -** Liquid Vault management via a personal device

This whitepaper describes the market need for the Liquid Vault, the Liquid Vault and its services, and the tokenomics of KIRO, the native utility token.

Market background

In only thirteen years, blockchain technology has created an ecosystem worth over $1.4 trillion. However, mass adoption of cryptocurrency remains a dream until some significant hurdles are overcome. We focus on three problems:

1. There are too many ways to irreversibly lose digital assets

2. Exchanges are either custodial or expensive

1. Loss of assets

It is too easy for crypto users to lose their digital assets, and it is a common occurrence.

To give a sense of scale: in 2018, digital forensics company Chainalysis estimated that there were 2.3-3.7 million lost bitcoins, worth $147– 236 billion at the time of writing. And that's just Bitcoin, which although the most valuable cryptocurrency is but one of thousands. And this was several years ago. In short, the true value of lost assets is far higher.

Ways to lose money include entering the wrong destination address when making a transfer (by mistake or by fraud), by losing the private key to a wallet, and by not making arrangements prior to death.

Losses are final because blockchain technology is by definition immutable. Erroneous transactions cannot be reversed. In addition, the pseudonymity of blockchain technology means that it is very difficult to identify malicious actors.

As a result, many cryptocurrency users seek safety in centralized solutions. But custodial applications create a different kind of risk – theft by hackers. In addition, centralization is contrary to the purpose of cryptocurrency: a world in which people have complete control of their own money.

2. Exchanges

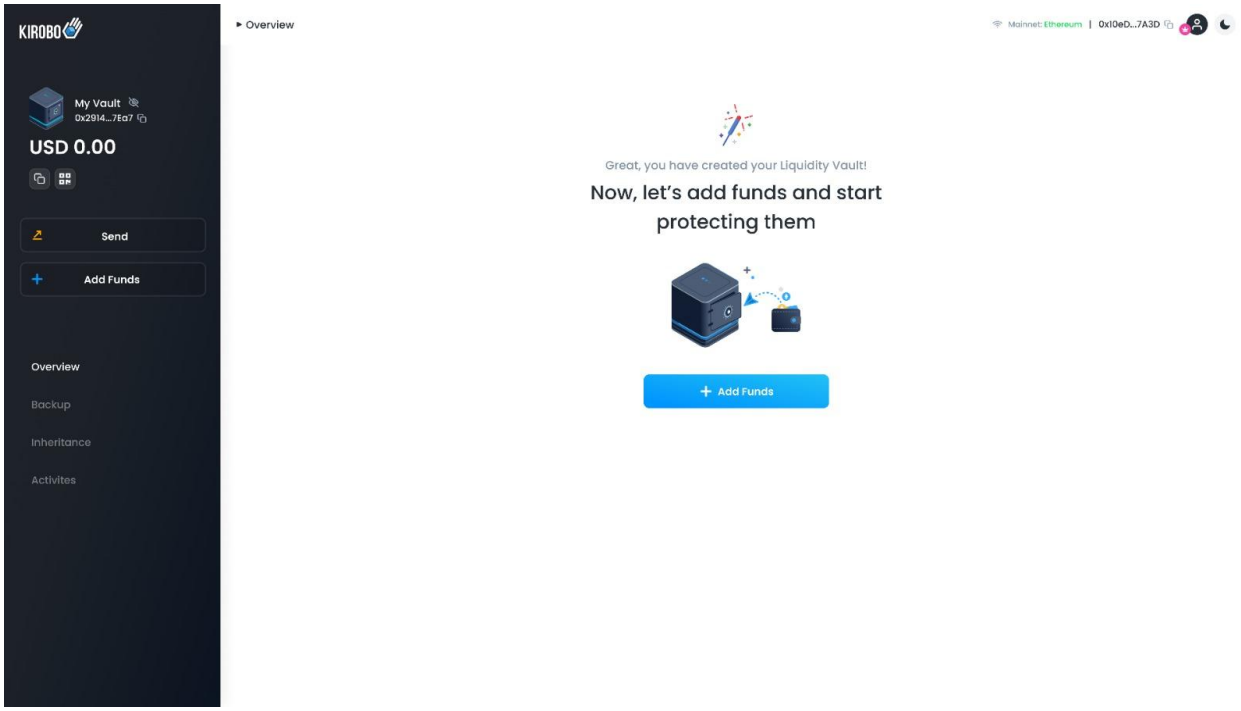
The majority of market trading volume takes place on centralized exchanges because they are easy to use and offer high liquidity. However, centralized exchanges are custodial and require KYC data, creating a target for hackers.

Decentralized exchanges provide a non-custodial alternative but present a different issue: slippage. Users lose money when conducting swaps via a DEX because the act of making the deal alters the balance of the shared trading pool, and thus the price of the tokens. And the more that is swapped, the bigger the discrepancy.

Billions of dollars of cryptocurrency are traded on crypto exchanges of both types every day - there is a real market need for a better solution.

The Liquid Vault

The Kirobo Liquid Vault is a non-custodial, decentralized, on-chain wallet with integrated applications creating an all-inclusive DeFi operations platform. All operations are decentralized, powered by the community by paying and receiving rewards in KIRO, the native utility token.



Liquid Vault dapps

Backup

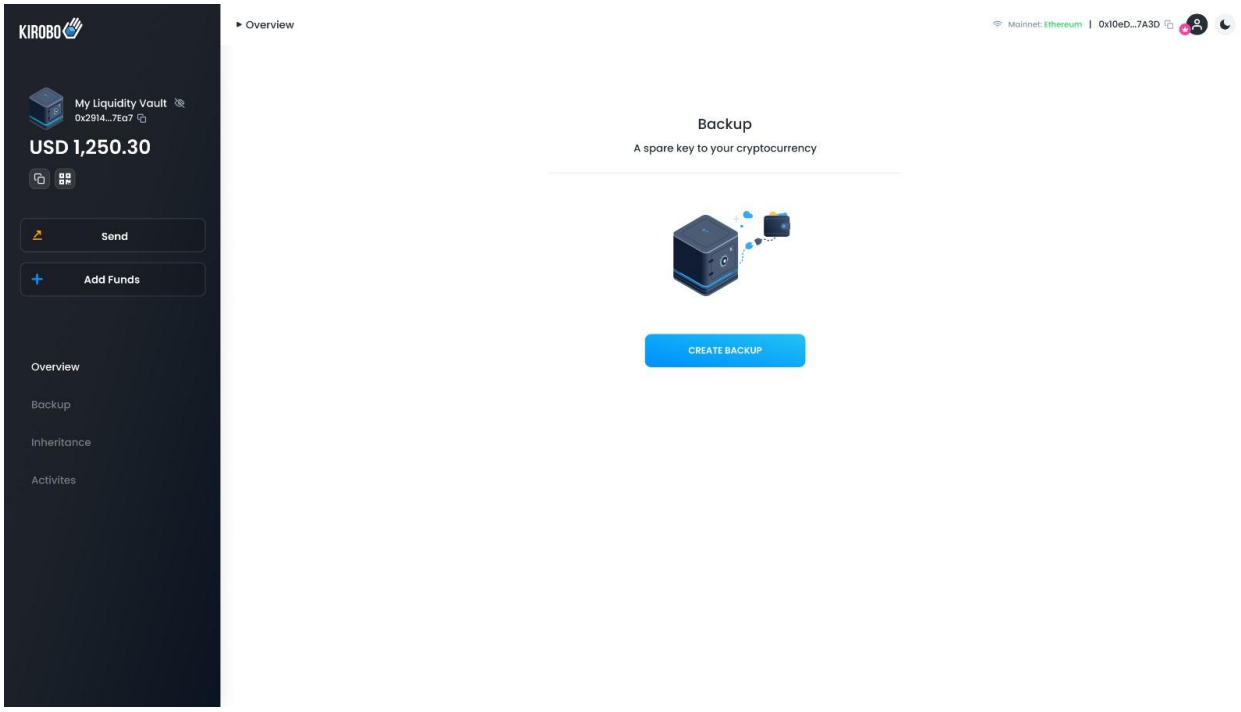
Background

Ownership of the contents of a cryptocurrency wallet is defined by a person's ability to access that wallet. This is because that wallet is the only way to access that part of the blockchain. If a person loses or forgets the access credentials - private key, password, seed phrase – the assets in the wallet are irreversibly lost.

Kirobo backup solves the issue of private key loss by enabling you to set up an automatic transfer of ownership of your Liquid Vault wallet to a backup wallet in case of inactivity. The user's vault thus has three access points – directly, via their external wallet, and to a third external wallet to which access will automatically be transferred if they do not reset the timer.

How it works

Setting a backup involves defining a secondary wallet and setting a timer via the interface:



Setting the backup timer requires a small amount of KIRO, and to activate the backup the user must deposit a certain amount of KIRO into the smart contract. The user may retrieve this stake whenever they like, but they're motivated to remain – first by the assurance provided by the system, and secondly by economic benefits as described in the tokenomics section.

When the timer reaches zero, a random system activator will be alerted and will activate that user's backup by sending a transaction to the smart contract. The smart contract transfers access to the inactive wallet defined by the user. When this

happens, that user's activation stake will be distributed throughout the ecosystem, as described in the tokenomics section.

Inheritance

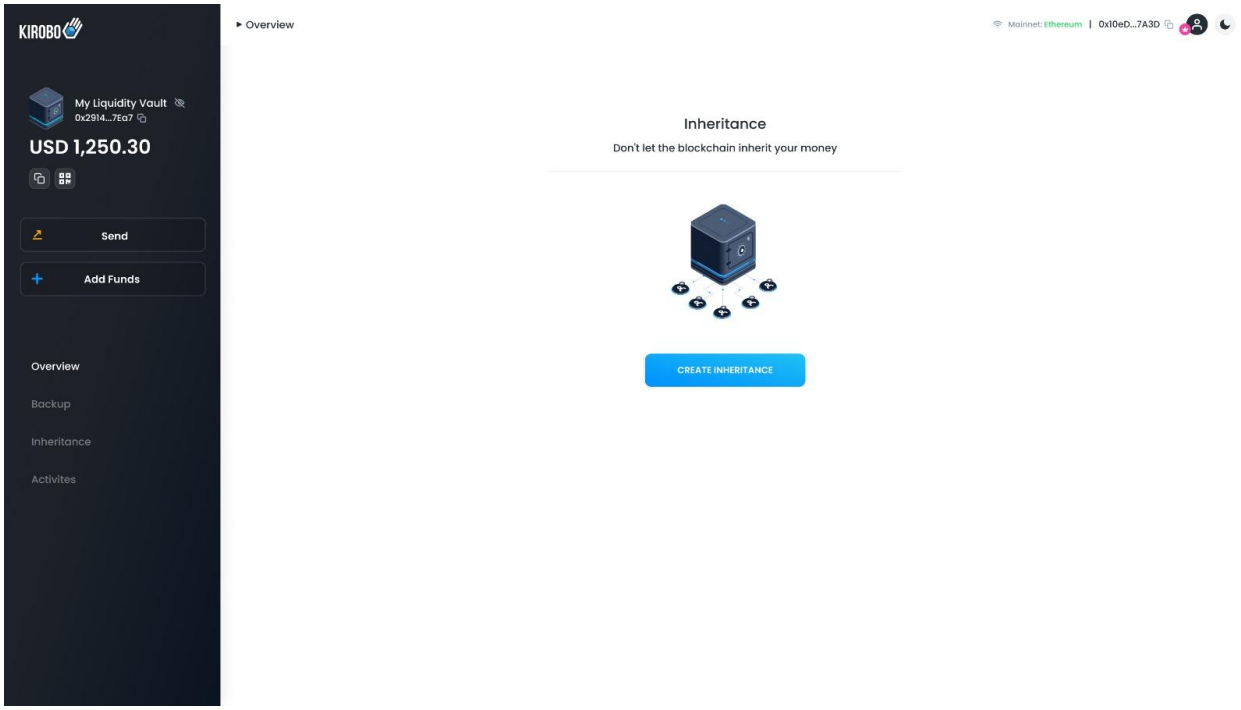
Background

If a person dies without leaving a will, their fiat assets will never be left unused. This is not the case with cryptocurrency. There are no authorities that will appropriate unallocated assets because there's no way to access them if the key is lost with the deceased. Cryptocurrency is just thirteen years old, but this is already a problem, and it's set to become increasingly relevant as the years progress and adoption of crypto increases. It's easy to imagine a custodial solution, but none can be entirely safe.

Kirobo inheritance is a non-custodial mechanism enabling users to bequeath assets to loved ones by pre-defining automatic transfers to up to eight different locations. Powered entirely by smart contract, there is no need to entrust your assets to anyone. Inheritance transfers can also be protected with Safe Transfer, preventing mistakes.

How it works

Setting the inheritance involves defining crypto wallets representing heirs, defining the amount each is to receive, and setting the timer via the interface.



Setting the inheritance requires a small amount of KIRO, and the user must periodically reset it, also for a small fee. To activate the inheritance, the user must deposit a certain amount of KIRO into the smart contract. The user may retrieve this stake whenever they like, but they're motivated to remain – first by the assurance provided by the system, and secondly by economic benefits as described in the tokenomics section.

When the timer reaches zero without being reset, a random system activator will be alerted and will activate that user's inheritance mechanism by sending a transaction to the smart contract.

When this happens, that user's activation stake will be distributed throughout the ecosystem, as described in the tokenomics section.

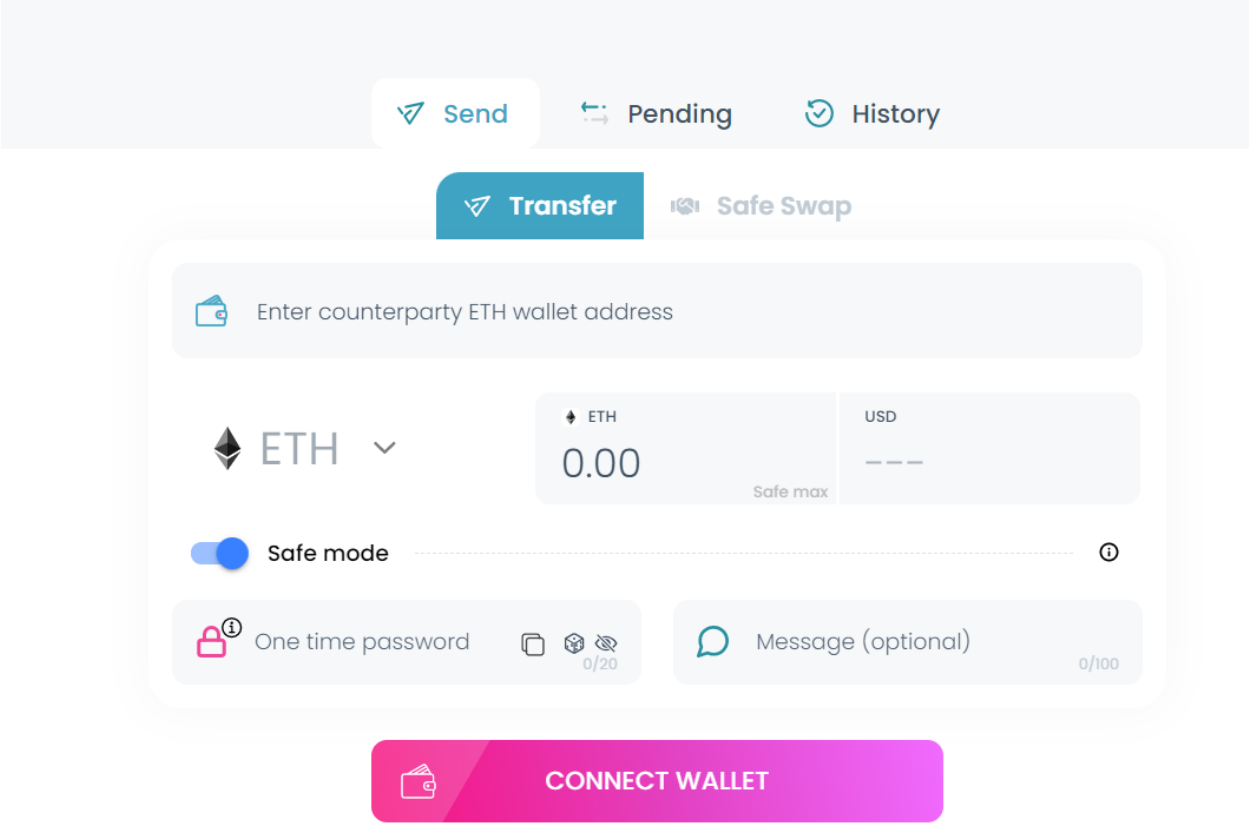
If the transfers were protected by Safe Transfer, the heirs will receive a notification and must enter the correct password to receive the assets. This is another vital layer of protection against human error.

Safe Transfer

Background

Mistakes are easy to make when sending cryptocurrency transactions. Wallet addresses are long strings of random characters that are not easy to recognize or feasible to remember. Copying an incorrect address is a common mistake, and if an address is replaced by a scammer, it is easy to miss. Furthermore, when a mistake is made, there is no recourse.

Kirobo's Undo Button is a non-custodial solution that effectively prevents cryptocurrency being sent to the wrong address by mistake or by fraud.



The sender sends the transfer but locks it with a password. The recipient must enter the password to collect a pending transfer. The sender can 'undo' the transaction and retrieve the assets at any time until the correct password is entered. The password is communicated independently of the system, so the possibility of sending money to the wrong address is prevented.

How it works

When a transaction is initiated, the sender's device transmits the transaction data, authentication key, and optional personal message. The authentication key is created by the sender's device and comprises the passcode created by the sender, a public salt, a private salt, and hash values derived therefrom. The authentication key is sent to the smart contract and the two salt values, transaction data, and personal message to the Kirobo server. The Kirobo server sits outside the blockchain.

The server then sends to the recipient's device the transaction data, a message if the sender chose to write one, and the public salt. Visible to the recipient is a pending incoming transaction and the message. When the recipient enters the passcode (received from the sender independently of this mechanism), their device will combine it with the public salt to create a hash value which is sent to the server. The server verifies the passcode by combining this hash with the private salt and hashing the resulting value. If valid, this will recreate the authentication key originally provided by the sender's device. In this case, the server will tell the smart contract to 'collect', and the transaction will be actioned.

In this way, the passcode alone is insufficient to validate the transaction, so that, for example, if communication of the passcode was intercepted or overheard, the imposter would not be able to collect.

Note that the service is entirely non-custodial. If Kirobo was hacked, pending transactions would be safe, and retrieval would still work.

P2P Safe Swap

Background

Token swaps made via decentralized exchanges are heavily affected by slippage, so that users do not receive a fair price for their tokens.

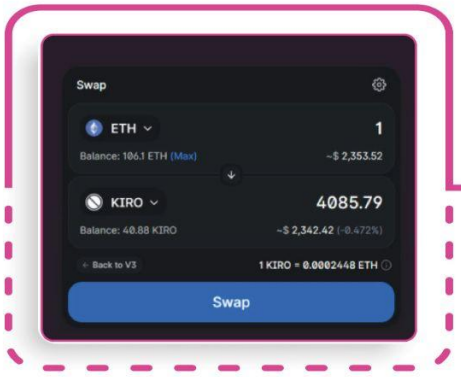
P2P Safe Swap enables users to execute simultaneous, passcode-protected peer-to-peer swaps, without risk of mistakes. As a result, they are able to set their own prices, avoiding the slippage characteristic of exchange venues.

About slippage

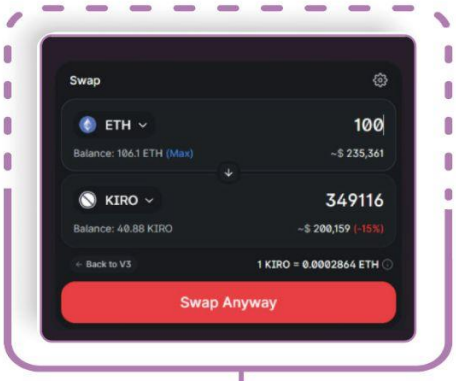
Slippage is the difference between a token's market price and the price at execution. Slippage on DEXs is high because trades are funded by pools. Depositing and withdrawing alters the balance of a pool - for example, trading 100 ETH for token n drives the price of token up, so the user gets fewer ns than they should. This also means that the larger the trade, the higher the slippage.

The user wants to swap 1 ETH for KIRO.
Assuming 1 KIRO = 0.5722 USD,
they receive 4,085.79 KIRO.

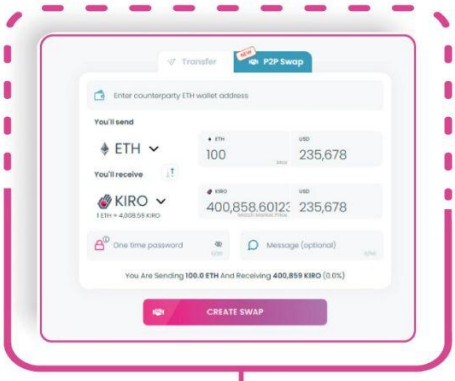
So 100 ETH should get them 408,579 KIRO.
But...

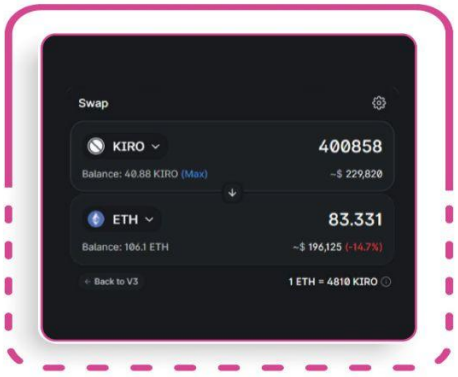


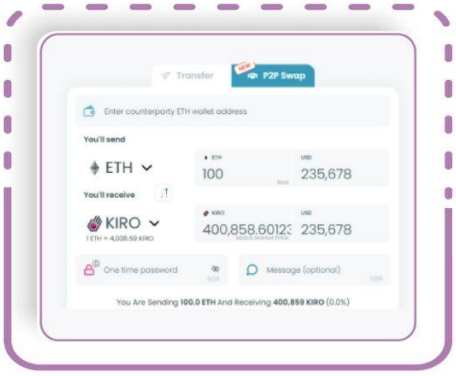
...here we see that they're only offered
349,116 KIRO - a loss of
34,024 USD.



The P2P Swap Button gives them
400,858 KIRO - saving them 34,024 USD.



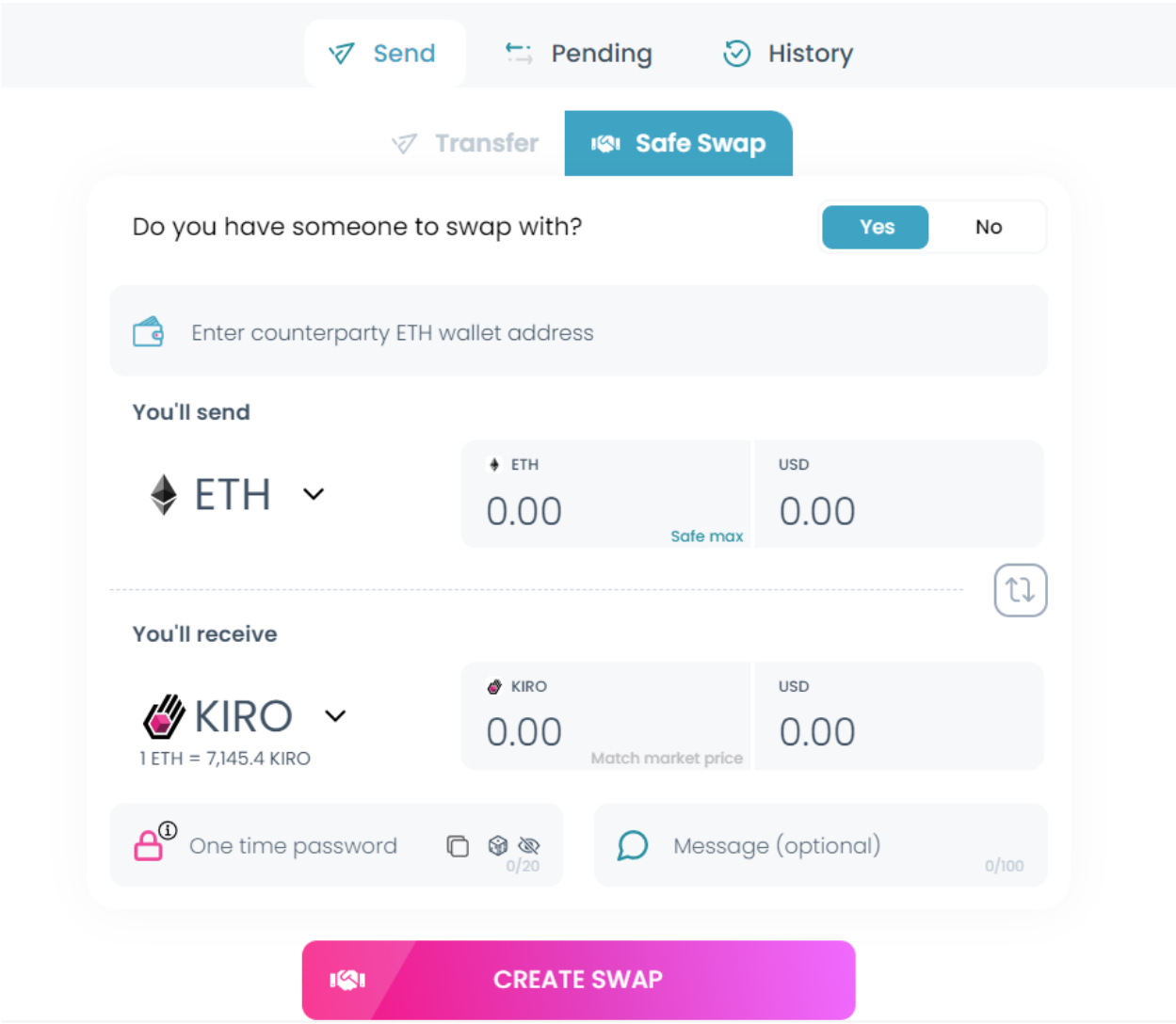




The second party also benefits, receiving the full 100 ETH instead of only 83.3 ETH.
That's a saving of approx. 44,000 USD.

How it works

The user enters the parameters of the trade - both tokens, the desired price of both sides of the transfer, the address, and the password. They then select create swap.



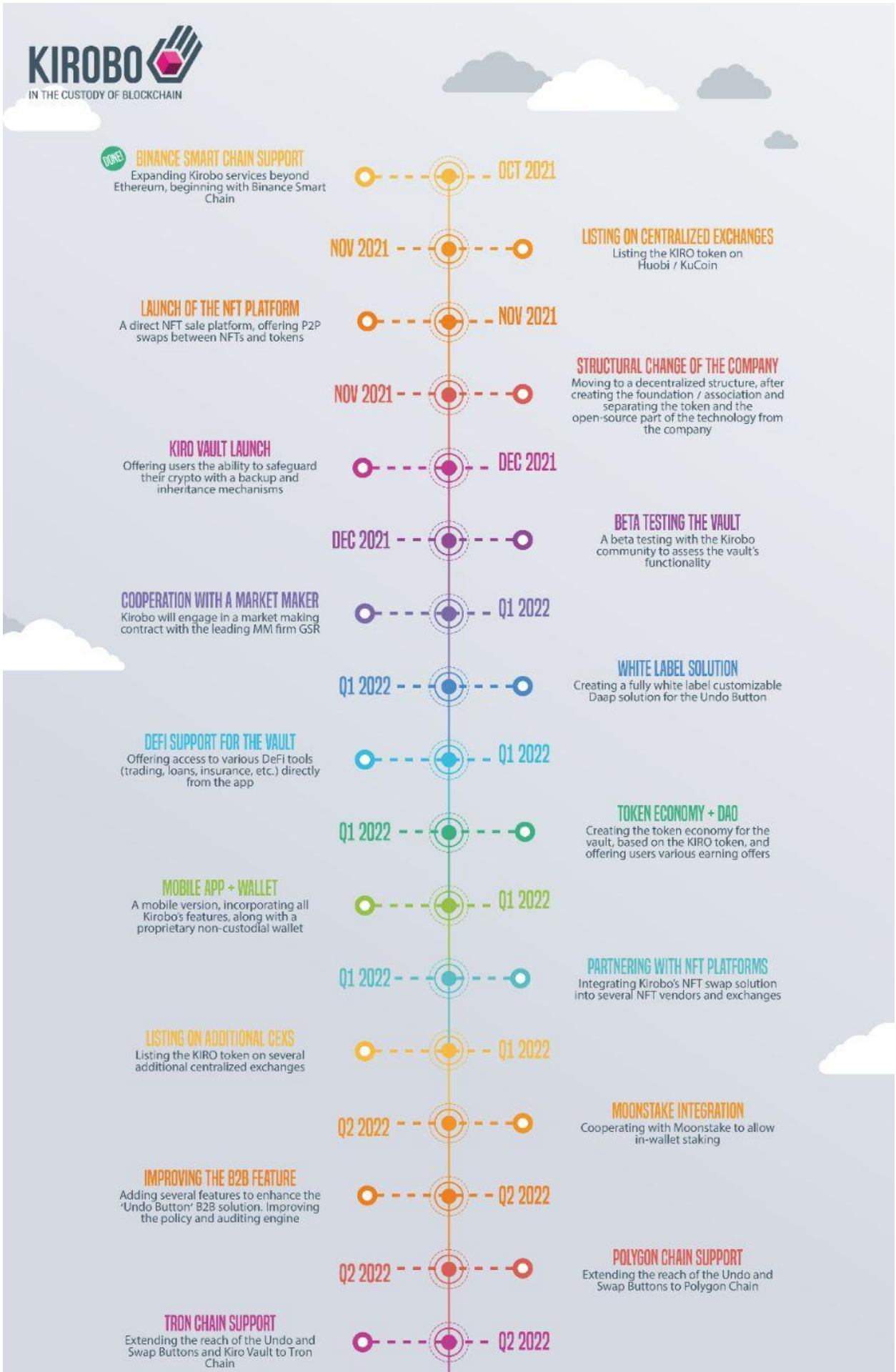
The second party reviews the transaction and enters the password. The smart contract collects from both wallets and deposits them in the other simultaneously.

As with the Undo Button, the initiator of the swap can cancel and retrieve their funds until the second party has entered the correct password, and the password is communicated independently of the system. The first party can cancel the transaction at any time until the second party enters the correct passcode and signs the transaction.

KIRO tokenomics

Text to come

Roadmap


KIROBO
IN THE CUSTODY OF BLOCKCHAIN
DONE!
BINANCE SMART CHAIN SUPPORT
Expanding Kirobo services beyond Ethereum, beginning with Binance Smart Chain
OCT 2021
NOV 2021
LISTING ON CENTRALIZED EXCHANGES
Listing the KIRO token on Huobi / KuCoin
LAUNCH OF THE NFT PLATFORM
A direct NFT sale platform, offering P2P swaps between NFTs and tokens
NOV 2021
NOV 2021
STRUCTURAL CHANGE OF THE COMPANY
Moving to a decentralized structure, after creating the foundation / association and separating the token and the open-source part of the technology from the company
KIRO VAULT LAUNCH
Offering users the ability to safeguard their crypto with a backup and inheritance mechanisms
DEC 2021
DEC 2021
BETA TESTING THE VAULT
A beta testing with the Kirobo community to assess the vault's functionality
COOPERATION WITH A MARKET MAKER
Kirobo will engage in a market making contract with the leading MM firm GSR
Q1 2022
Q1 2022
WHITE LABEL SOLUTION
Creating a fully white label customizable Daap solution for the Undo Button
DEFI SUPPORT FOR THE VAULT
Offering access to various DeFi tools (trading, loans, insurance, etc.) directly from the app
Q1 2022
Q1 2022
TOKEN ECONOMY + DAO
Creating the token economy for the vault, based on the KIRO token, and offering users various earning offers
MOBILE APP + WALLET
A mobile version, incorporating all Kirobo's features, along with a proprietary non-custodial wallet
Q1 2022
Q1 2022
PARTNERING WITH NFT PLATFORMS
Integrating Kirobo's NFT swap solution into several NFT vendors and exchanges
LISTING ON ADDITIONAL CEXS
Listing the KIRO token on several additional centralized exchanges
Q1 2022
Q2 2022
MOONSTAKE INTEGRATION
Cooperating with Moonstake to allow in-wallet staking
IMPROVING THE B2B FEATURE
Adding several features to enhance the 'Undo Button' B2B solution. Improving the policy and auditing engine
Q2 2022
Q2 2022
POLYGON CHAIN SUPPORT
Extending the reach of the Undo and Swap Buttons to Polygon Chain
TRON CHAIN SUPPORT
Extending the reach of the Undo and Swap Buttons and Kiro Vault to Tron Chain
Q2 2022

Summary: creating a decentralized infrastructure

Blockchain technology is growing in use, but its lack of user-friendly, secure, and economic services are a barrier to mass adoption. The Liquid Vault provides decentralized services of a standard comparable to those associated with fiat finance. Kirobo presents non-custodial methods for people to protect their assets, transact safely, safeguard access to themselves and their loved ones, and take advantage of a user-powered ecosystem to increase their holdings.

Kirobo solutions will encourage mass adoption of cryptocurrency, moving the world towards a fairer, people-powered future.

Appendix - Undo Button for Bitcoin

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. Furthermore, the disclosed embodiments do not require additional transactions to "reverse" the original transaction, 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 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 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.