LEIOS

Technical Paper

Authors: Ara Arakelyan; Zorayr Zakaryan
Editor: Soheeb Aziz; KJ Magill

v5.0
10.14.2018

Overview

Leios International, Inc. (Leios INC) is a company that aims to be the most practically usable block chain-based fund transfer system for a mass-scale of global users. The idea is to replace the current blockchain interface with one familiar to the average consumer, with features expected by those simply looking for a better fund transfer solution, and not a speculative investment. Ultimately, Leios will replace the need for people to face the volatility of cryptocurrency price fluctuations while maintaining its decentralized advantages. In order to achieve this, Leios will operate in conjunction with a stablecoin to allow for a system of fund transfer in the equivalent of fiat. Leios will also privatize transactions to remove the undesirability of a public display of personal funds, while complying with global KYC regulations to allow for legal operations in all markets. Finally, Leios will provide methods of exchange between fiat and stablecoins, and thus will essentially become a decentralized method to globally transfer fiat in a way superior in price, and potentially in speed, to all current transf er methods.

Technical Goals

The goal of Leios INC is to devise a system that addresses all of the common disincentives which the average user finds in current cryptocurrency fund transfer implementations. These are the five critical improvements Leios brings:

1. Provide a familiar username-based simple account management with full privacy (see Section 2 of Specifications).
2. Develop an untraceable high-throughput blockchain protocol enabling private transactions (see section 3 of Specifications).
3. Protect the user from exchange rate volatility by implementing stablecoin atomic swaps (see section 5 and 6 of Specifications).
4. Create ways to facilitate seamless fiat-crypto exchange through a network of Leios partners positioned around the globe, and potentially allowing for point-of-sale transactions (see section 6 of Specifications).
5. Provide our simplified and privacy-enhanced experience to be applicable to all cryptocurrencies supported by atomic swaps (see section 7 of Specifications).

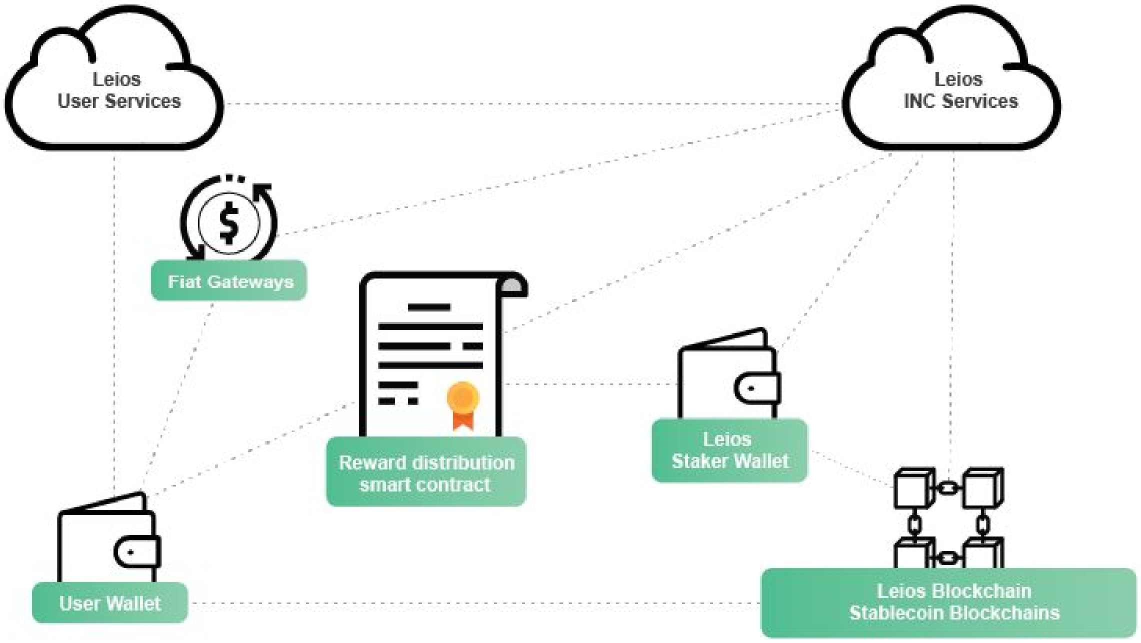
Specifications

1. Overall Scheme

The main features of the system are:

1. Secure and localize wallets for each user. Only users will have access to their private keys, leaving any components of trust with third party keystores entirely up to them, with no involvement from Leios INC.
2. Facilitate all transfers to be private, preventing anyone from tracing individual transactions, including Leios INC, while maintaining KYC regulations internally.
3. Enable users to hold their funds in the form of stablecoins like DAI, BitUSD, and others to avoid price volatility.
4. Facilitate LEIOS token holders to lend their tokens (through reward-based staking) in order to support private transactions.
5. Create transparent fee collection and distribution among stakers powered by public smart contracts.
6. Ensure that any faltering of service or downtime cannot harm users and stakers or their funds.

There are several components that work in conjunction within the Leios system to support fiat deposit, withdrawal, internal funds transfer, staking, and reward distribution. Below is a visualization of component interaction:



Leios Blockchain

Leios will have its own blockchain to support private and almost costless transactions of the LEIOS token. Participants in the Leios system can use atomic swaps for private funds transfers.

Fiat Gateways

External gateways to support fiat<->stablecoin transactions and to allow fiat deposits and withdrawals for Leios users.

Leios INC Services

A cloud-based service to support staking, reward distribution, and market-making for the LEIOS token and any stablecoins used within the system.

Reward Distribution Smart Contract

Transparent smart contract to store the collected fee-based rewards for stakers and to distribute it among them periodically.
of emerging technologies which we wish to take advantage of, yet we still want a built-in mechanism to allow LEIOS INT to switch to a better version of these technologies in the future.

Leios User Services

A cloud-based service to support a user search function in mobile and web applications without compromising privacy. The service does not store or receive any sensitive data, including public wallet addresses of users.

User Wallet

Mobile or web application to securely store different wallets and participate in transaction signing for atomic swaps and transfers.

Leios Staker Wallet

Mobile or web application to control the staking - practically, it can be a part of the user wallet.

2. Mobile Wallet

The Leios mobile Wallet (or application) is one of the main components of the Leios system, because it is responsible for securely holding funds and signing required blockchain transactions.

Nowadays, with cryptocurrency still very much in its infancy, the general user interface of blockchains are hardly intuitive enough for the average user. In order for cryptocurrencies to represent a reasonable alternative to fiat currency wallets, simplifications must be made in the initial access to cryptocurrency assets, as well as the workflow required for making transactions.

We believe that exposing aspects of public-key cryptography as ubiquitous as a public key deter the average user from committing to using a cryptocurrency transaction system. Verifying the identity of the receiver, a step that should be as streamlined as possible for daily usage, becomes a source of constant uncertainty and hassle for non-technical users. The evident nature of this problem can be seen in the existence of proposals such as EIP928 for address avatars on Ethereum. In order to bridge the differences between conventional and blockchain transactions, Leios INC believes that a pas

sword, fingerprint, and pin-based interface for the authentication of the Mobile Wallet is the best solution to facilitate users of all levels of technical expertise.

Here is the list of features and components of the mobile application:

a. Intuitive UI for general users who are not familiar with crypto-world. Android and iOS devices will be supported.
b. Unique username-based account in the Leios network, and the ability to search others by username.
c. Local secure sign-in using user preferred options including password, pin, Face ID, and fingerprint.
d. Intuitive KYC completion processes in order to deposit or withdraw fiat.
e. Multiple payment methods integration for fiat deposits and withdrawals.
f. Securely stored Leios, stablecoin, and other crypto wallets.

g. Hardware encryption for wallets if OS and device are supported, hence allowing the Leios app to be hardware wallet replacement.
h. Ability to stake Leios tokens by sending them to Leios temporarily, and generate rewards based on the staking amount.
i. Transaction signing to support crypto transfers and to participate as a party in atomic swaps.
j. Protection against external screenshots, rooted installs, keylogging, and other types of attacks.
k. User-attached public and private keys (u-key) to sign, encrypt, and decrypt data when communicating with external Leios services.
l. Wallets and user data backup methods including QR codes, NFC, mnemonics, and external trusted services.
m. Advanced options to facilitate interaction with cryptocurrency-related services such as depositing/withdrawing crypto.

3. The Leios Blockchain

In order to enable the core functionality of the Leios platform—namely efficient transfers of fiat-equivalent value between users—there must be a blockchain that has the following properties:

- Fast transactions
- Negligible or non-existent fees
- Private transactions
- Proven security void of attack vectors
- Fixed supply of tokens

To support all these features, a new blockchain will be developed based on Komodo technology. The following is an explanation of the key features and their reasons for implementation:

Short block times: Aside from the convenience of instantly receiving funds, this is also necessary in order to eliminate the minutes of suspense that normally elapse in many blockchain transfers before one can see their funds have been sent or received.

Z-addresses: This is one of the components of Komodo which the Leios Blockchain will inherit to usen order to ensure all transactions are private, and the sending source cannot be viewed on a publically accessible ledger. This also prevents Leios INC from keep a record of specific transactions. Leios INC will, however, have a separate record of verified users to ensure compliance with KYC AML requirements, at the direction of our ongoing legal guidance.

DPoW security mechanism: This is to root the security of the Leios Blockchain into other proven PoW networks. Leios INC believes in focusing on proven and secure measures for all transfers, in order to eliminate any possible risk to any users of the blockchain.

Atomic swap compatibility: The ability to automate the exchange of different blockchain assets is the key component of the Leios system. Atomic swaps allow for the Leios Blockchain to act as an intermediary between stablecoins and other crypto assets in order to facilitate several of the key components of the system:

- The inclusion of private transactions onto any stablecoin or other atomic-swap compatible cryptocurrency.

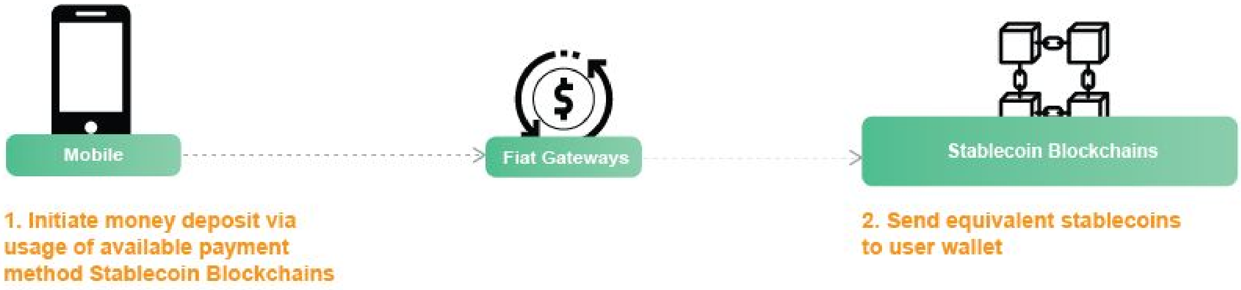
- The ability to hold stablecoins or cryptocurrencies of other blockchains in the Leios app while allowing Leios to manage their actual transfer through the Leios Blockchain.

- The inclusion of an automated point of payment from Leios users to Leios INC and the providers of the LEIOS tokens that facilitate the transaction.

- The ability to initiate a transaction in one stablecoin and conclude it in another. This will allow for stablecoin interoperability and choice flexibility. This feature can potentially be extended to all atomic-swap compatible cryptocurrencies in the future.

4. Deposit/Withdrawal

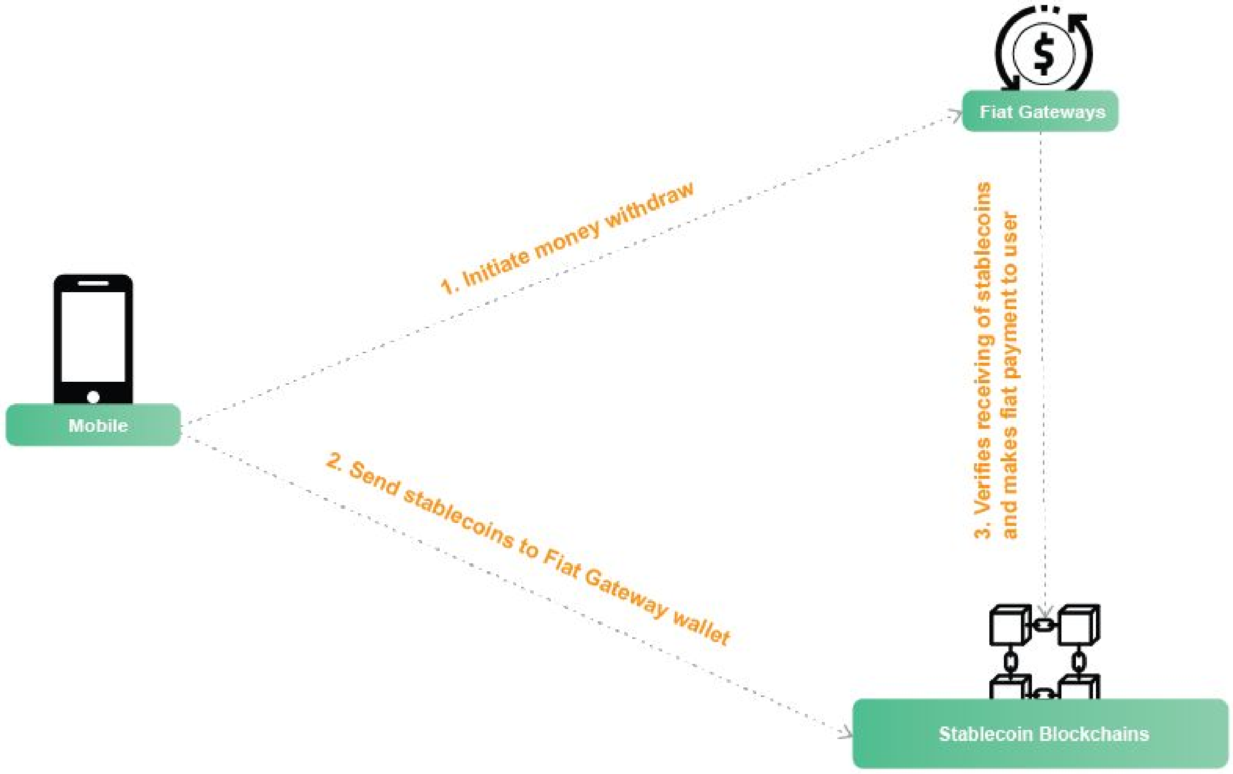
In order to initiate a transfer of funds, the user must first deposit their funds to their mobile wallet, which can be done according to the following diagram:


Mobile
Fiat Gateways
Stablecoin Blockchains
1. Initiate money deposit via usage of available payment method Stablecoin Blockchains
2. Send equivalent stablecoins to user wallet

1. In the first step, the user will deposit their fiat via a Fiat Gateway available in their country. The mobile application will allow the user to use any payment method provided by the appropriate Fiat Gateway and make the deposit. During payment, the user will also provide his stablecoin wallet public address.
2. After user performs the payment, the Fiat Gateway will the send equivalent amount of stablecoin to the user's stablecoin wallet. A fractional percentage of the payment will be taken by the Fiat Gateway as a fee, differing by location.

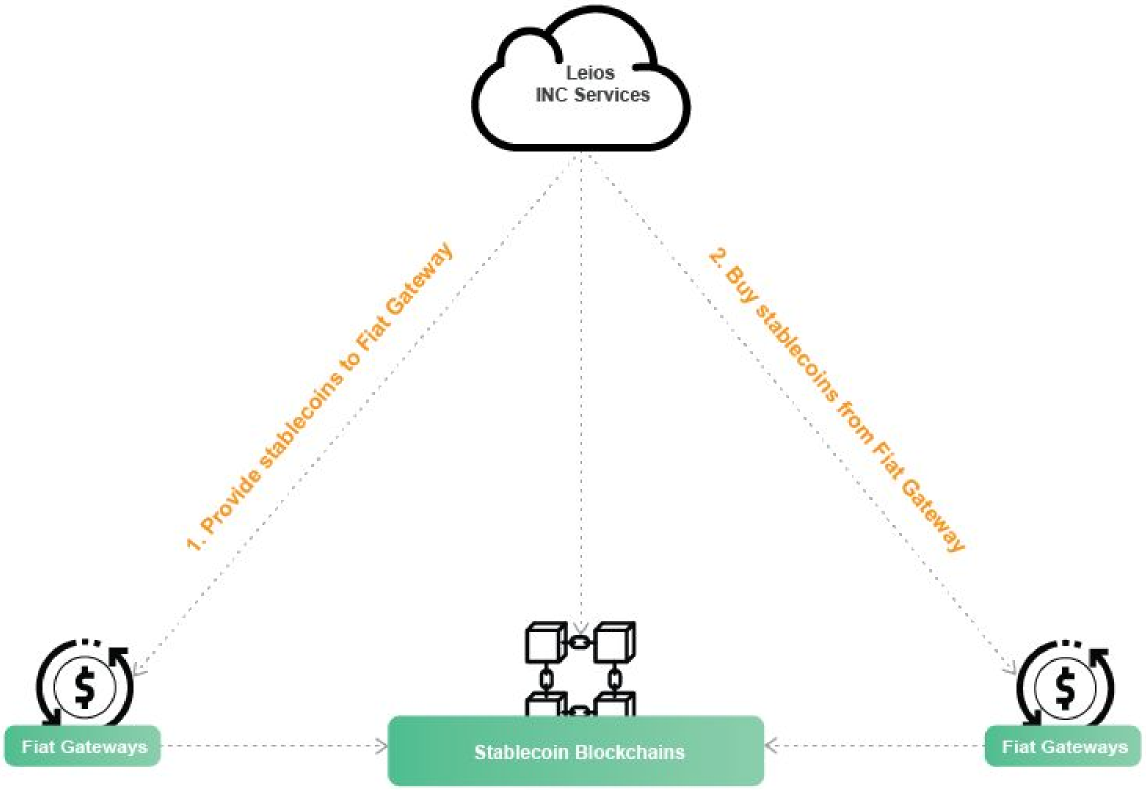
From the above diagram we can see that the funds are kept in stablecoins in a mobile wallet, which protects the user from any volatility in the cryptocurrency market.

At any time, the user can withdraw their stablecoins via the appropriate Fiat Gateway available in their country. The Leios System will initially only facilitate the withdrawal of stablecoins received via the process of money transfer described in Section 5.3. Withdrawals will be done according to the following schema:


Fiat Gateways
1. Initiate money withdraw
Mobile
2. Send stablecoins to Fiat Gateway wallet
3. Verifies receiving of stablecoins and makes fiat payment to user
Stablecoin Blockchains

1. During the first step, the user's mobile application will initiate money withdrawal via the appropriate Fiat Gateway's API call, which will return to the user's Fiat Gateway stablecoin wallet address.
2. The user then sends the stablecoins he wants to withdraw into fiat to the Fiat Gateway (using the wallet address received in the previous step).
3. Finally, the Fiat Gateway verifies receiving of stablecoins and performs fiat payment to the user. Some percent of stablecoins will be taken by the Fiat Gateway as a fee.

Leios INC takes part in circulation of stablecoins between them and the Fiat Gateways according to the following diagram:


Leios
INC Services
1. Provide stablecoins to Fiat Gateway
2. Buy stablecoins from Fiat Gateway
Fiat Gateways
Stablecoin Blockchains
Fiat Gateways

1. In order for the Fiat Gateway to have enough liquidity for the necessary stablecoins (which are needed when users want to deposit money to their mobile wallets), Leios INC will always provide enough stablecoins to the appropriate Fiat Gateway (through our internal arrangements with the Fiat Gateway), using our pre-planned stablecoin liquidity pool that will always be kept at a larger amount than the highest estimations of the demand.
2. Leios INC will always buy back its stablecoins from Fiat Gateways, which they have received from users during withdrawing of fiat funds in their local currencies, hence allowing Leios INC to restart the cycle with new users.

Through agreement with our exchange partners, Leios INC will fix the price of stablecoins with exchange partners at 1 USD per coin. This will ensure a predictable cycle with precise fee calculations from entry to exit, ensuring consistency throughout the price of the USD equivalent stablecoin to actually match USD at all stages possible. This will eliminate even the minor volatility found in the stablecoin market.

5. The Transfer Process

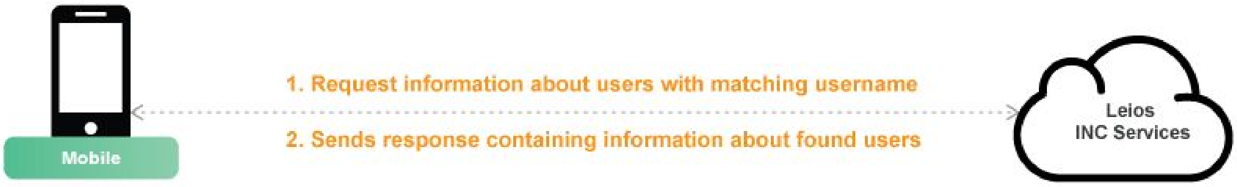
In order to fully understand the stages of transfer, each stage of the transfer process will be explained through an example from a hypothetical transaction, from its initiation to completion.

For the this section, let us suppose Alice wants to transfer $100 worth of stablecoins from her wallet to Bob's. The money transfer process consists of three phases described in the subsections below: searching of target user, confirming the transfer by target user, and the actual money transfer process. After initiating the money transfer process via the mobile application, Alice must enter the amount she wants to transfer (in our example, $100) whereafter she will be redirected to the user search screen.

5.1. User Search

In order to start the money transfer process, Alice must firstly find the target user whom she wants to send money to. She can do this via the user search screen of the mobile application by entering a name (or part of a name) for the target user. The mobile application will perform a user search according to the following diagram:

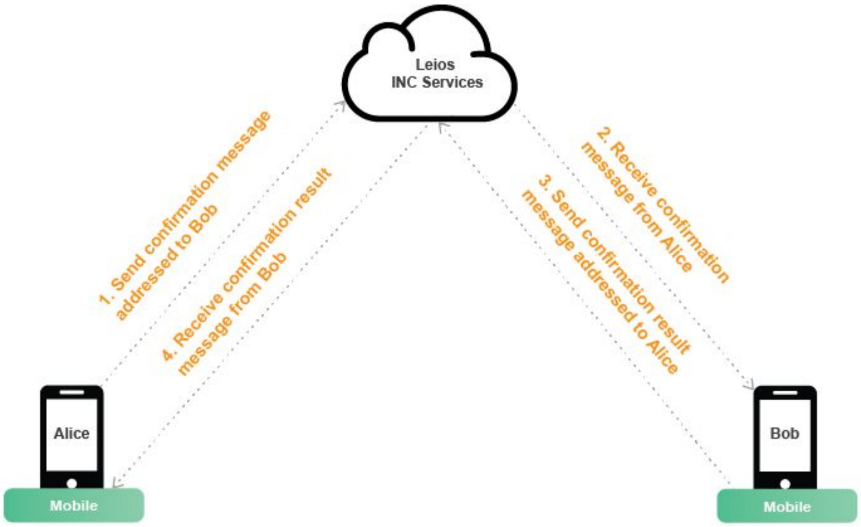
1. The mobile application will send a user search request to Leios Services containing search text entered by Alice.
2. Leios Services will find users with matching usernames and send back response-containing information (username and attached public u-key, which is generated for confirmation purposes) about each found user.


Mobile
1. Request information about users with matching username
2. Sends response containing information about found users
Leios
INC Services

After receiving the search results, Alice must choose her intended target user (in our example Bob) and initiate the process of money transfer confirmation.

5.2 Confirmation

Alice cannot start the money transfer process until receiving a confirmation from Bob. The confirmation process will be done according to the following diagram:


Leios
INC Services
1. Send confirmation message addressed to Bob
4. Receive confirmation result message from Bob
2. Receive confirmation message from Alice
3. Send confirmation result message addressed to Alice
Alice
Mobile
Bob
Mobile

1. During first step, Alice's mobile application prepares a special confirmation message addressed to Bob, and sends that message to Leios Services. The body of the confirmation message contains the transfer ID, the amount of money going to be transferred, and the username and public u-key of initiator (i.e. Alice). The digital signature of Alice (which is constructed using Alice's private u-key) is appended to the body, then the final message is constructed by encrypting the result using Bob's public u-key. The final message can only be decrypted by Bob (using his private u-key), hence only allowing Bob to see that Alice wants to send him money. After constructing the final message, Alice's mobile application sends it along with information about the message recipient (Bob's username) to Leios Services, then waits to confirm the result message from Bob. If, after some predefined time, Alice does not receive it (or cannot receive it due to being offline), the money transfer process will be rejected.

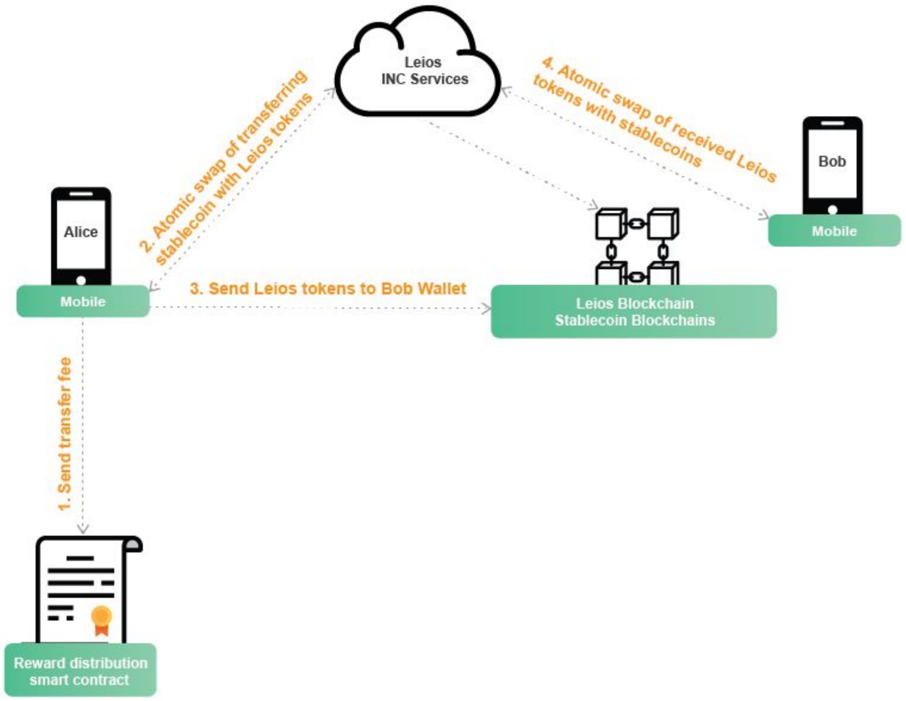
2. In the second step, Bob will receive the message addressed to him. Bob can only receive it if he is online; otherwise, after some time, the entirety of the transfer will be rejected, as mentioned in the previous step. After receiving the message, Bob's mobile application will decrypt it using his private u-key. From the body of the message, it will be relayed that: the message relates to money transfer confirmation, the amount of money to be transferred, and the information about the transfer initiator (i.e. Alice's username and public u-key). After this, the digital signature will be verified (using Alice's public u-key) in order to confirm that the message was really sent by Alice. If everything is executed properly up until this step, then the mobile application will prompt Bob to confirm the transfer of $100 coming from Alice.
3. During the third step, Bob will confirm or reject the money transfer from Alice, prompting Bob's mobile application to prepare the appropriate result message addressed to Alice and sending that message to Leios Services. The body of the result message contains the transfer ID (found in the first message coming from Alice), username and public u-key of receiver (i.e. Bob), and the

public address of Bob's Leios wallet, where Bob is to receive the transferred LEIOS tokens (for details, please refer to Section 5.3). The digital signature of Bob (which is constructed from Bob's private u-key) is appended to the body, and then the final message is constructed by encrypting the result using Alice's public u-key. The final message can only be decrypted by Alice (via usage of Alice's private u-key), hence only Alice can see if Bob rejects or confirms her money transfer. After constructing the final message, Bob's mobile application will send it paired with information about the message recipient (Alice's username) to Leios Services.

4. During the last step, Alice will receive a message addressed to her (on the condition that she is online, as mentioned in the first step). After receiving this message, Alice's mobile application will decrypt it using her u-private key. From the body of message, it will be relayed that the message is related to the result of money transfer confirmation with the specified ID, along with the information regarding the message sender (i.e. Bob username and public u-key). After this, the digital signature will be verified (using Bob's public u-key) in order to guarantee that the confirmation result message was actually sent by Bob. The mobile application will show the confirmation result to Alice ("Transfer Rejected" or "Transfer Confirmed"). If the transfer was rejected, then the whole process will be interrupted. If confirmed, the money transfer phase will automatically be started.

5.3 Transfer

The money transfer process will be done according to the following diagram:


Leios
INC Services
2. Atomic swap of transferring stablecoin with Leios tokens
4. Atomic swap of received Leios tokens with stablecoins
Alice
Mobile
Bob
Mobile
3. Send Leios tokens to Bob Wallet
Leios Blockchain
Stablecoin Blockchains
1. Send transfer fee
Reward distribution
smart contract

All transactions initiated in the blockchain will be signed locally in order to keep the wallet private keys local for the purpose of concealing them from anyone but the owner. The process will require the initiator of the transaction to be online in order to sign the transaction.

1. In the first step of the money transfer, Alice's mobile application will initiate the transaction of sending the required fee amount of the transfer to the Reward Distribution Smart Contract. For example, when initiating the transfer of $100, then $0.25 in the equivalent of the fiat-representing stablecoin will be sent to the Reward Distribution Smart Contract. This means the transfer amount is $99.25 (equivalent stablecoins), with a 75 cent fee on top.

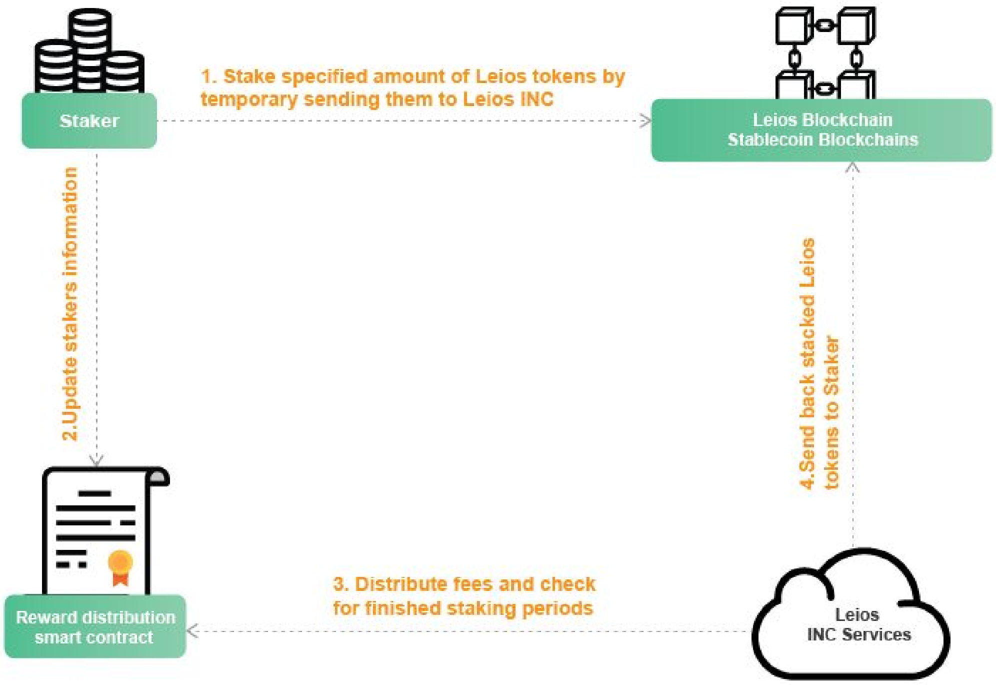
2. During the second step, Alice's mobile application will perform atomic swaps to exchange the stablecoins with an equivalent value of Leios tokens. The second party of atomic swap will be Leios INC, which will always have enough liquidity of Leios tokens (Explained in Section 6). After the atomic swaps, Alice will have Leios tokens in her Leios wallet that she must send to Bob's Leios wallet. Her mobile application has obtained Bob's wallet public address during the fourth step of the Confirmation phase.

3. During the third step, Alice's mobile application transfers her Leios tokens to Bob, for which zero-knowledge transaction capabilities of the Leios blockchain will be used in order to keep the money transfer untraceable between Alice and Bob.

4. Now that Bob has received Leios tokens in his wallet, the next step is exchanging them for stablecoins. In order to do this, Bob's mobile application initiates atomic swaps with Leios INC to swap his Leios tokens with stablecoins. The second party of the atomic swap will again be Leios INC, which will always have enough liquidity for the stablecoins. After performing this step, Bob will see $99.25 transferred into his wallet. If Bob is offline after the completion of the third step, then the last step will be performed as soon as Bob is online again.

6. Staking

Any user who owns LEIOS tokens can stake them to be used in the second step of the money transfer process (for details, please refer to Section 5.3). As a reward for their role in providing LEIOS liquidity, stakers will periodically receive a percentage (according to amount of provided Leios tokens) of the transfer fee to their wallets. Staking is performed from the mobile application according to the following diagram:


Staker
1. Stake specified amount of Leios tokens by temporary sending them to Leios INC
Leios Blockchain
Stablecoin Blockchains
2.Update stakers information
4.Send back stacked Leios tokens to Staker
Reward distribution smart contract
3. Distribute fees and check for finished staking periods
Leios
INC Services

1. The staker initiates the staking process in the first step via the mobile application by specifying the amount of Leios tokens which they are going to stake, along with the time period of staking. The staking amounts and time frame will be published using smart contracts to ensure transparency for all stakings. Then the staker's mobile application will generate the transaction into the Leios Blockchain to send the specified amount of Leios tokens to Leios INC. Leios INC will then use these tokens in order to create enough LEIOS liquidity to participate in the atomic swap transactions described in Section 5.3.

2. In addition to sending LEIOS tokens to Leios INC, the staker's mobile application also updates the Reward Distribution Smart Contract by adding information about the staking and the specified amount of LEIOS tokens for the specified time.

3. This distribution step is periodically performed by Leios INC for two reasons. The first is for the distribution of collected fees (in stablecoins) among all stakers along with the portion for Leios INC. The second reason is to check the staking periods for registered stakings. Any expired stakings will be removed from the Reward Distribution Smart Contract.

4. After finding an expired staking, Leios INC will also send back the staked Leios tokens to the staker to whom it belongs. They will be sent to to the Leios wallet of the staker by initiating the appropriate transaction in Leios blockchain.

7. Extending Privacy to other Other Blockchain Assets

Upon completion of our mobile and web applications, and the Leios blockchain, users can theoretically send any cryptocurrency or blockchain-based asset that is supported by atomic swaps through our network. It would simply require us to integrate the wallets for these cryptocurrencies into our applications in the same manner that we integrate our preferred stablecoins. A user can then login to their account and find options to send and receive these cryptocurrencies, same as with our fiat representative stablecoin.

Just as with our stablecoin, these cryptocurrencies will be atomically swapped into LEIOS and then swapped again into their original currency on their receiving end. This will allow for the transactions of any cryptocurrency to now enjoy the same privacy network that we created for the Leios token and the stablecoins it supports.

The integration of non-stablecoin as USD representatives opens the door for the application to be a useful one to those familiar with blockchain, but is incompatible with our target remittance and other fund transfer users. Therefore, Leios INC will create an advanced version of the application for those interested in applying the privacy and general streamlined transactions to other cryptocurrencies. We can link these cryptocurrencies to our network of fiat gateways to allow for users to acquire or sell them with ease in supported location.

Conclusion

Given the recent surge in cryptocurrency development, many new modifications to the original idea of Satoshi Nakamoto have emerged, all of which aim to add something to the versatility and usability of blockchain technology. We believe that the time has come to select the most casual, user-friendly elements that have emerged and combine them into a single system; one that solely exists to have maximum usability at a mass-scale level. An simple-to-interact-with blockchain system, a user-friendly interface, and an externally-run system to bypass fiat-related restrictions. These elements will combine to create the ideal union between fiat and cryptocurrency for everyday fund transfers.

Leios will eliminate any learning curve needed to use cryptocurrency and combine the familiarity of traditional e-finance with the unique advantages of blockchain. The successful implementation of this system will give overwhelming incentives to move beyond slower, more expensive methods available to anyone who uses traditional fund transfer services. These advantages do not require the user to have any interest in using or understanding blockchain or cryptocurrency. The system will gain widespread adoption solely based on its own merits of convenience and cost-reduction, perhaps being the first real bridge between blockchain as a technology and general consumer adoption.