# Unnamed: UTXO-Like Wallet For Algorand

*Liquid Glass*

*liquid.glass.drops@gmail.com*

## 1. Introduction

There are two types of blockchain data structures, namely the account model and the UTXO model. The latter is used in cryptocurrencies like Bitcoin and Cardano, while the former is used in cryptocurrencies like Algorand and Ethereum. While the account model is good for cryptocurrencies where its blockchain can handle smart contracts, it suffers from two main issues, which is its vulnerability to phishing attacks and privacy. A UTXO model-like wallet is implemented as a solution to the mentioned problems related to cryptocurrencies that uses the account model as it lessens the reliance on one account. However, cost can be an issue if there are too many addresses.

## 2. Advantages of Account-Based Ledgers

Account-based ledgers are usually meant for blockchains that has smart contract functionalities. For example, Algorand, where you have DApps like Tinyman,  Algofi, Algorand Name Service, to name a few. States in these types of ledgers are being treated as an account, where values are changed based on its transactions. This makes transactions easier when interacting with smart contracts as there is only one account to query balance from.

Account-based ledgers also allows an identity to be associated to an address. This makes signing in to certain sites like Unstoppable Domains with your wallet possible.

## 3. Issues With Account-Based Wallets

Address reuse has two main problems. Firstly, reusing an address means that all of the balance in an address will be compromised in the event where the private key is compromised like phishing, where you unknowingly key in your seed phrase to a phishing website. Secondly, since your identity is tied to an address, anyone who has your address are able to view your transaction history and your savings.

## 4. Advantages of UTXO-Based Ledgers

UTXO-based ledgers allows for more privacy as balances are not tied to one address and it is spread across many addresses provided that a new address is generated for every transaction. Think of addresses like a hundred dollar note. An address contains a fixed value and unlike account-based ledgers, balance in terms of arithmetics does not exist in terms of UTXO. If an address is spent, you are giving the whole value to another address and there is no possibility of splitting the value into any other values but instead you receive a change, which is the balance that is sent to a new address. And since every transaction uses a new address, compromising all of the private keys becomes more difficult provided that the master key is not compromised.

## 5. Issues With UTXO-Based Wallets

Using UTXO in the context of smart contracts is inefficient as querying balance becomes very difficult due to multiple addresses present. Cardano's implementation of Extended UTXO uses stake keys to keep track of balances across multiple address but it reduces privacy as a stake key on the blockchain explorer will be able to show all of the associated addresses and the overall balance.

Electrum uses Hierarchical Deterministic wallets that generate new addresses using a master private key. While this is good for privacy, it is less secure due to the fact that all of the address is being generated from a master key.

Cost can be an issue with UTXO-based ledgers as too many addresses can lead to higher transaction fees.

## 6. Solution

An implementation of a wallet that has the benefits of privacy and security in UTXO-based walletss and the capability to isolate addresses to interact with DApps like an account-based wallet is possible but such implementation cannot be done on-chain as the blockchain has already implemented an account model. Every address shall be generated using a newly generated BIP 39 seed phrase for every transaction in case the user needs to manually enter the seed phrase for whatever reason.

To keep the implementation simple, the Algorand Python SDK is used as it has functionalities like generating keypairs and sending transactions.

It is highly recommended that after a few address is generated, the balance should be consolidated in a new address to prevent the need to maintain many keypairs.

## 7. Users

Users are less likely to have all of their assets compromised due to the fact that different seed phrases are used. By generating a new keypair for every transaction isolates the keypair in the event of a phishing attempt.

For merchants who are using Algorand as payment, you may want to use this wallet to prevent phishing and maintain some level of privacy while allowing the transactions to be as public as possible.

## 8. Conclusion

By having an Algorand wallet that has the UTXO model capabilities can help prevent phishing and maintain an acceptable level of privacy by using new keypairs generated using the Algorand Python SDK while having the ability to isolate a keypair just for DApps only.

## 9. References

1. https://www.horizen.io/blockchain-academy/technology/expert/utxo-vs-account-model/
2. https://en.bitcoin.it/wiki/Address_reuse
3. https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
4. https://github.com/algorand/py-algorand-sdk