Unnamed: An Algorand Wallet That Mimics UTXO

Liquid Glass

liquid.glass.drops@gmail.com

1. Introduction

Traditional methods of digital payments through credit or debit cards require submitting the relevant information in order to be able to do a transaction which can be a good thing when it comes to ensuring that there is an actual identity tied to the card. However, when unsuspecting users are interacting with malicious actors, these information that are shared willingly can be used to spend on things without the card holder's knowledge. This can be negated by taking precautions when doing online transactions like reading the URL carefully and check if the website is malicious or not but such actions are not only inconvenient, but also rely on the willingness of taking such precautions or even if they are taught to take such measures in the first place.

Most cryptocurrencies of today that has Decentralized Applications (Dapps for short) uses a public ledger and reuses a single address. While this is good for transparency, there must be a way for users to be able to choose on whether if they want their identities to be tied to that transaction or not.

To encourage the adoption of cryptocurrencies, transactions must be private and secure at the same time without having to sacrifice convenience.

2. Privacy

When using Dapps, reusing address is needed as certain actions like signing and approving transactions will have its history recorded. In this case, reusing addresses would allow the Dapp to record your activity, therefore making your account eligible for an airdrop for example.

However, we can limit the reuse of an address to just one Dapp by isolating an address for every Dapp, therefore giving the Dapp user a choice to stay private without sharing any extra details about themselves if needed.

In other scenarios like incoming and outgoing transactions that involves transferring of assets from one address to another does not require reuse of address as transactions are only done once and have no reason to keep it. Such transactions should be using a new address for every single transaction as this not only reduces the likelihood for anyone not involved in the transaction to link your identity to an address.

3. **Disputes**

   When implementing privacy, we must not forget that we must also allow the intervention of authority figures when there is a need to. By using a different address on a public ledger, we are trying to unlink our identity from an address whose transaction that is already made public and anyone can see it but there will still be traces of someone's identity tied to an address. A very good example of this would be chats on e-commerce platforms, where the seller will share their address to receive payment. Whenever there is a need to submit the transaction details, the address coupled with the seller's details should be submitted.

   Since the blockchian records all of the transactions that ever occurred and is immutable, sending the assets from an address whose identity has been tied to will be very difficult to unlink again. This means that it is not possible for anyone to be dishonest provided that there is evidence priving that the new address contains transactions with the assets in question.

4. **Security**

   There are cases where a wallet is drained of its assets due to a compromised private key, allowing transactions to be approved without the wallet owner's consent. This is very concerning when there is reuse of address involved as addresses are keypairs where every public key that has a corresponding private key, which is often stored on the computer, can be spent readily. By generating a new keypair, we are creating a sandbox, where every Dapp is limited to the balance of an address. That is, even if one keypair is compromised for whatever reason, only part of the assets will be fully spent, minimizing the extent of stolen assets.

5. **UTXO**

   The UTXO or Unspent Transaction Output model is used by Bitcoin to ensure that addresses

   are not used more than once to prevent double spending. Every unspent address upon spending will be fully spent regardless if there is a balance at the end. If there is balance as a result of the transaction, the balance will be moved to a newly generated address as a change that belongs to you while the outgoing transaction containing the required amount for payment goes to another newly generated address belonging to another person.

   This is useful in maintaining privacy and security as addresses are never used more than once by sending all of the balances to a new address, where the addresses are always going to be keypairs that are used once and never used again when spent.

   To be able to use the properties of UTXO on a ledger that uses an account model, the concept of double spending is not needed as there is no interaction of the ledger to query if an address belongs to a wallet.

   To find the total balance of the wallet, every addresses in a wallet are queried independently to find the balance and then added together while spending from every address requires concurrency when submitting transactions with the spent address removed from the wallet as the transaction history has already recorded the spent addresses involved in the transaction, therefore mimicking how UTXO works.

6. Conclusion

By reusing addresses in transactions that does not require address reuse harms the privacy of the user as identity can be linked easily to an address compared to using different addresses for every tranaction. The exception would be Dapps, where address reuse is a must, will have a new address generated just for that Dapp. This creates a sandbox mechanism where private details like identity will optionally be shared on one Dapp at a time and in the event where the private key is compromised, the extent of assets stolen will be limited. To be able to settle transaction related issues, privacy must be optional in this case where addresses with evidence that the address belongs to a certain identity must be submitted together to an authority figure. UTXO is a solution to address the issues surrounding public ledgers that encourages address reuse and therefore some aspects of UTXO should be mimicked in a wallet.

7. References

1. Wikipedia - “Unspent transaction output” (https://en.wikipedia.org/wiki/Unspent_transaction_output)
2. Horizen - “UTXO Vs Account Model” (https://www.horizen.io/blockchain-academy/technology/expert/utxo-vs-account-model/)
3. River Financial – “Bitcoin’s UTXO Model” (https://river.com/learn/bitcoins-utxo-model/)
4. GeeksForGeeks - “What is Unspent Transaction Output (UTXO)?” (https://www.geeksforgeeks.org/what-is-unspent-transaction-output-utxo/)
5. Address Reuse By Bitcoin.it (https://en.bitcoin.it/wiki/Address_reuse)
6. Hodl Hard - “4 Reasons Why Bitcoin Address Reuse Is Dangerous” (https://hodlhard.io/blog/bitcoin-address-reuse/)
7. Wasabi Wallet - “Risks Associated with Address Reuse” (https://blog.wasabiwallet.io/risks-associated-with-address-reuse/)
8. CNBC - “Ongoing solana attack targets thousands of crypto wallets, costing users more than $5 million so far” (https://www.cnbc.com/2022/08/03/hackers-attack-solana-crypto-stealing-millions.html)
9. CoinDesk - “Solana Wallets Targeted in Latest Multimillion-Dollar Hack” (https://www.coindesk.com/markets/2022/08/03/phantom-wallet-exploit-drains-millions-in-sol-tokens/)
10. Reddit – “Lost 17,000 $ of ETH due to hacked Metamask wallet” By u/madaye on r/ethereum (https://www.reddit.com/r/ethereum/comments/se017w/lost_17000_of_eth_due_to_hacked_metamask_wallet/)
11. Reddit - “How do crypto wallets get hacked? Very curious about this topic.” By u/ForbiddenOwl on r/AskNetsec (https://www.reddit.com/r/AskNetsec/comments/p9cxdw/how_do_crypto_wallets_get_hacked_very_curious/)
12. Phishing By TechTarget (https://www.techtarget.com/searchsecurity/definition/phishing)