

# Algorand Greenhouse Hack 3

By Liquid Glass  
<liquid.glass.drops@gmail.com>

Bring Your Own Project



# Introduction

- Unnamed is targeted at users who want:
  - Privacy
  - Security
- Unnamed mimics UTXO
  - Like Bitcoin
  - New address every transaction
  - Unlike HD Wallets
  - Generates non-related keypairs
- Unnamed does not modify how Algorand works



# Motivation

- Carousell
  - Rise of phishing attacks
    - Unsuspecting users entering payment card details
  - Targets
    - Merchants
    - Buyers
  - Thought: “If cryptos are used, only addresses are shared, making successful phishing attempts slightly harder but people will want privacy during a transaction”

# Motivation

- Why Algorand?
  - Low transaction fees (0.001 Algos)
  - Fast transaction finality (confirmation <5 sec)
  - High transaction throughput (6000 TPS)
  - Entice more e-commerce platforms and normal users to use Algorand by building wallets that grants privacy when transacting



# Motivation

- Privacy
  - Merchants and customers may not want transactions to be seen by everyone
  - However if there are any disputes, transactions must still be seen by authority figures when needed
  - In fact, every Algorand user deserves privacy

# Motivation

- UTXO
  - What is UTXO?
    - Originally proposed by Hashcash to make sure that digital payments can never be replicated
    - Bitcoin uses it
    - Every address is treated as states (spent / unspent)
    - Once spent, the all of the balance in the addresses involved is spent at once
    - Balance is sent to new address as change
    - The amount to be sent to be someone else will be sent to new address
    - Already spent addresses are checked to make sure that it is not spent again
    - No address reuse



# Motivation

- UTXO
  - Quote from Bitcoin's whitepaper:
    - "... but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous."
    - "As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner."
    - "Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner"

UTXO = Privately Public



# Motivation

- What About Account Model?
  - Address are treated as accounts
  - Arithmetics
  - Addresses are not states unlike UTXO
  - A special value is used once when submitting a transaction to prevent replication of the same transaction
  - Good for Dapps
  - Simple to implement
  - But reuse address

Address Reuse + Public Ledger = Weak Privacy



# Motivation

- What about security?
  - Case study 1: HD Wallets
    - All keypairs are generated from one master key
    - Easy backup
    - One (master) key compromised = all balances in every address spendable
  - Case study 2: Legacy (Non-Deterministic) Wallets
    - Every keypair is not generated from a master key
    - Harder to backup
    - One key compromised = one address spendable

# Solution: Unnamed

- What is Unnamed
  - Reverse engineered UTXO
  - Reimplemented some properties of UTXO
  - Mainly the privacy and security aspects
    - Preventing address reuse
  - Concurrency of outgoing transactions
  - Does not prevent replication of transactions
    - Algorand's account model does it for us
  - Does not modify how Algorand works



# Solution: Unnamed

- Unnamed will:
  - Generate a new wallet for you for every new transaction (Done - Before Hackathon)
  - Allow you to send all of the balance from every wallet easily (WIP - Testing)
  - Allow you to check all of the balance from every address as a whole (WIP)
  - Allow consolidation of all balances in the wallet either by choice or when sending (WIP)
  - Not use rekeying (Remember privacy with UTXO?)

# What About Dapps?

- Unnamed currently does not have Dapps in its timeline due to lack of expertise and time constraints
- Unnamed focuses on simple transactions for now



# Want To Help?

Unnamed welcomes devs who are willing to make Unnamed not only handle simple transactions but also the ability to use Dapps in a way that is private and secure

# Want To Help?

- Contact Liquid Glass
  - Gmail (Most Preferred)
    - [liquid.glass.drops@gmail.com](mailto:liquid.glass.drops@gmail.com)
  - Reddit
    - u/0xLiquid\_Glass
  - Gitcoin
    - 0xLiquidGlass
  - Twitter
    - 0xLiquidGlass



Thank You



# Credits & License

- Content by <Liquid Glass>  
<http://<https://github.com/0xLiquidGlass/unna-med>>  
 License: <GPL v3>
- OpenOffice.org template by Raphaël Hertzog  
<http://raphaelhertzog.com/go/ooo-template>  
 License: GPL-2+
- Background image by Alexis Younes “ayo”  
<http://www.73lab.com>  
 License: GPL-2+