



pw

Please install WALLETH 0.20





# WALLETH

The native Android Ethereum light client wallet

# 5 lenses:



User



Developer



Attacker



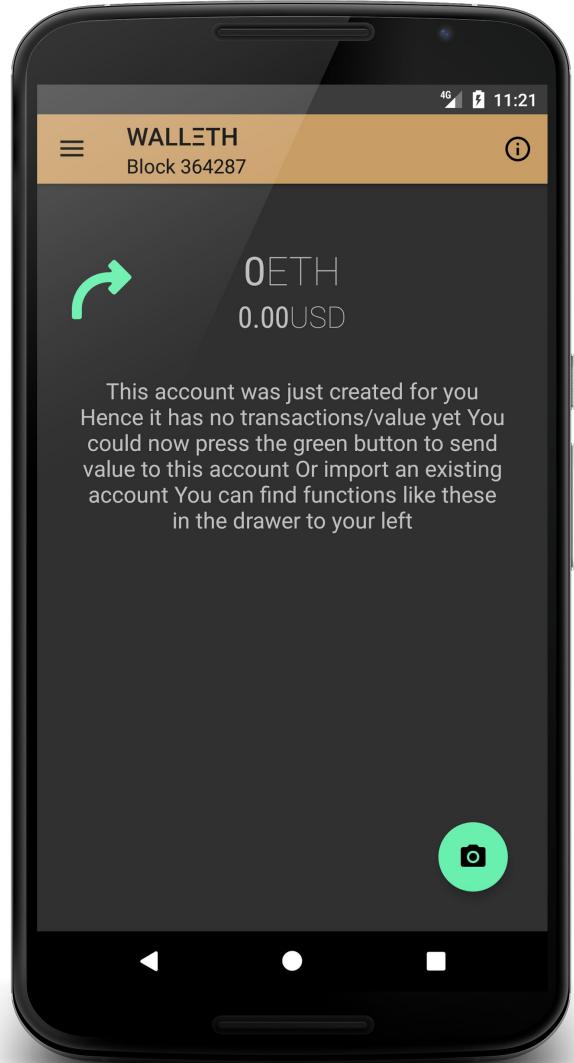
Wide angle

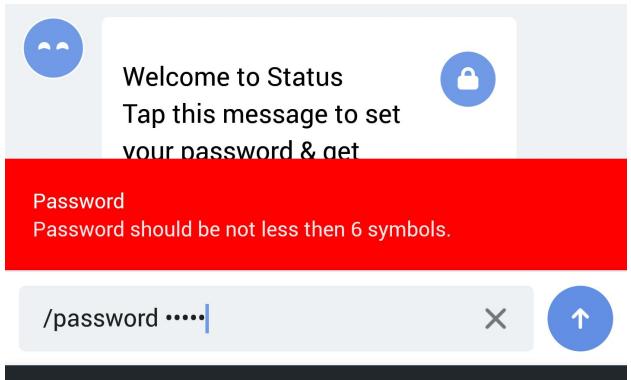
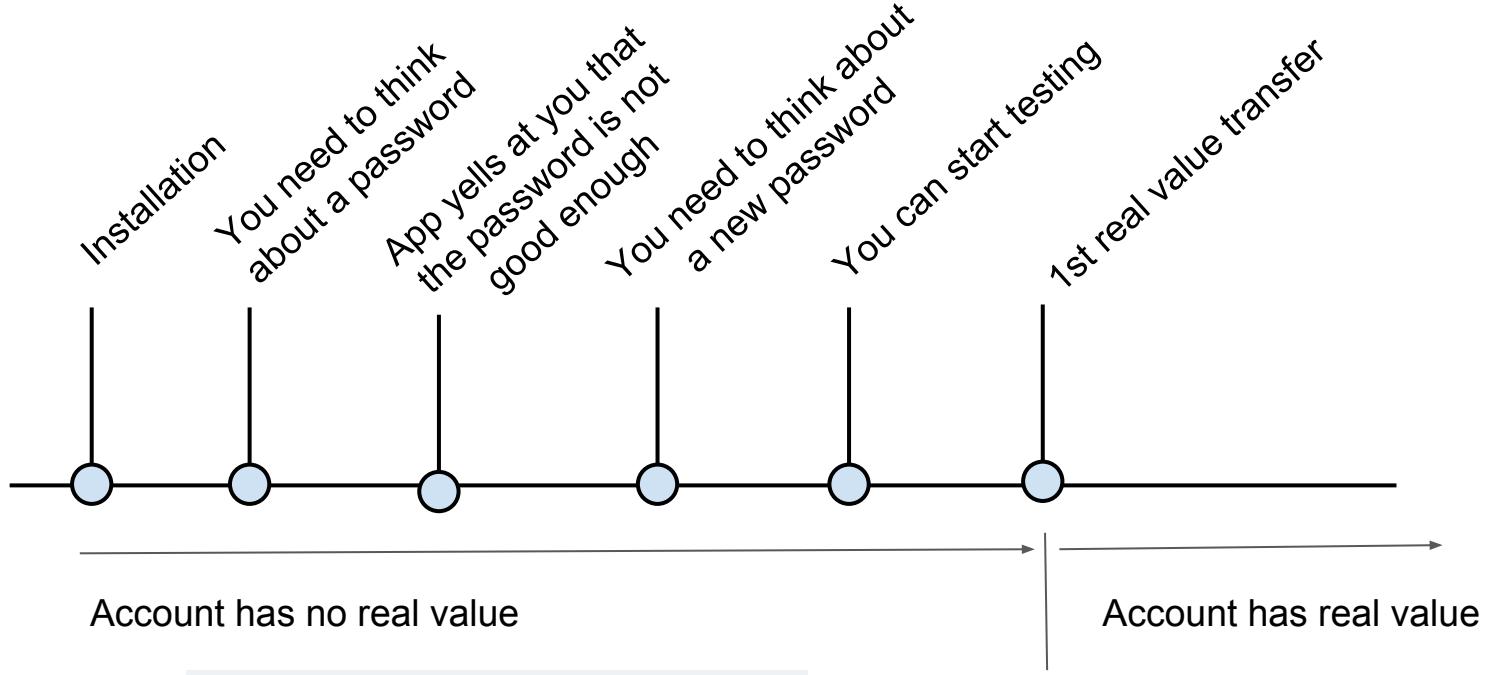


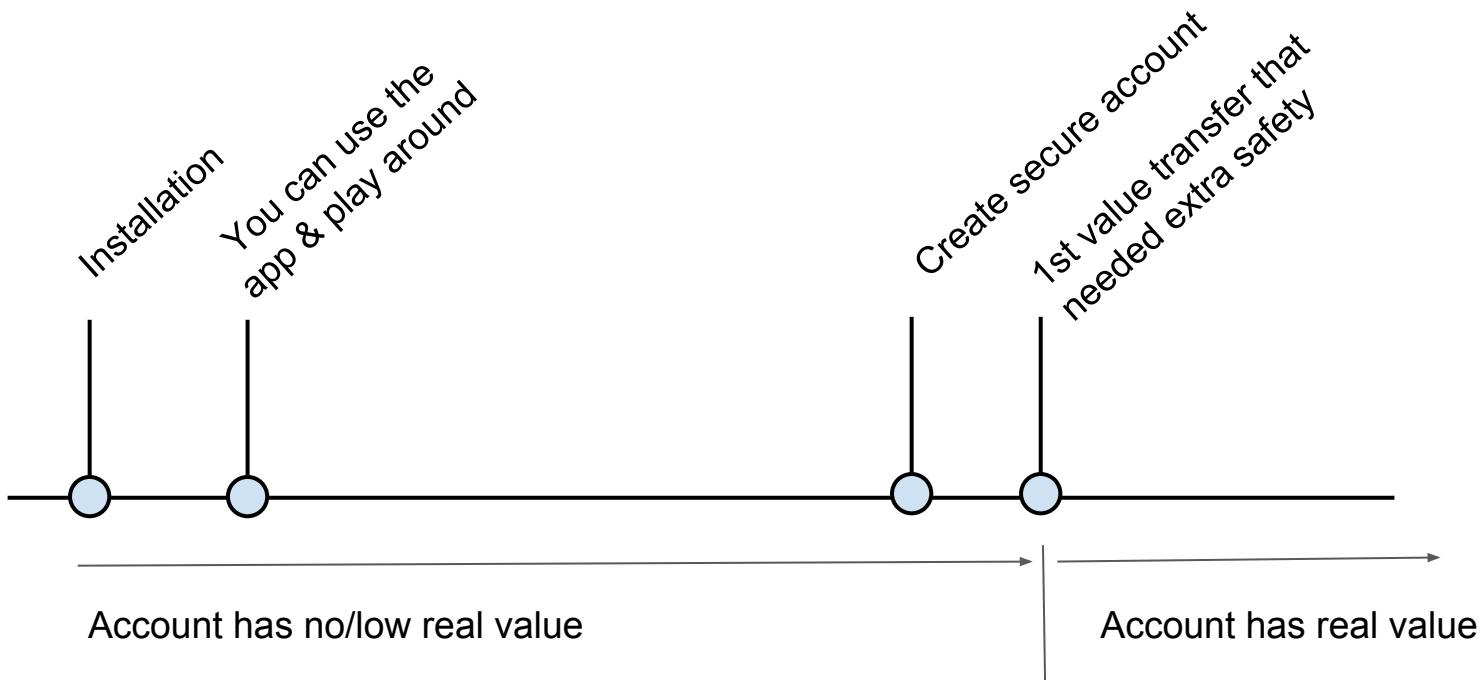
Yours

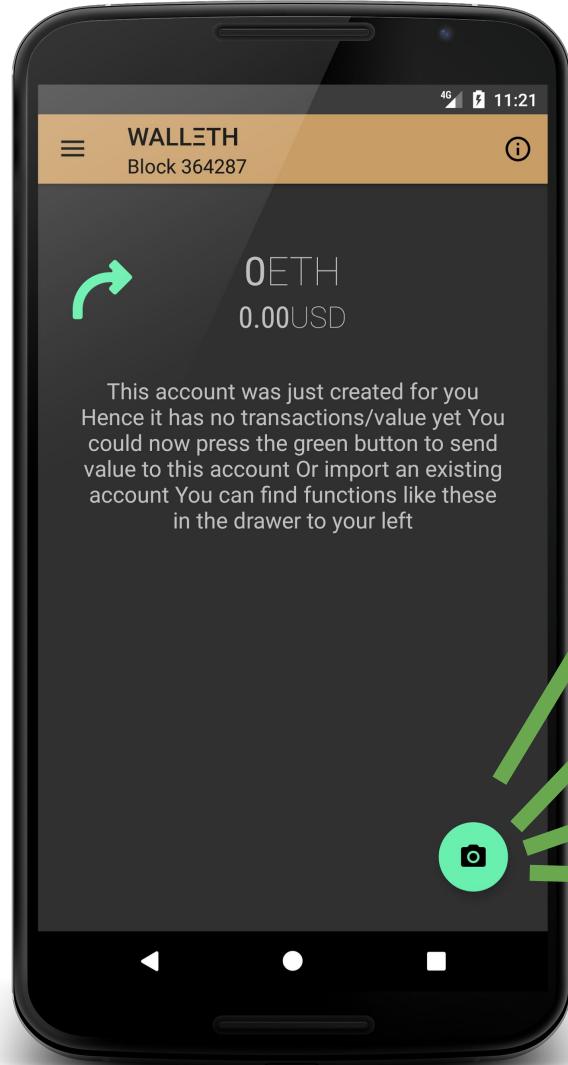


# User









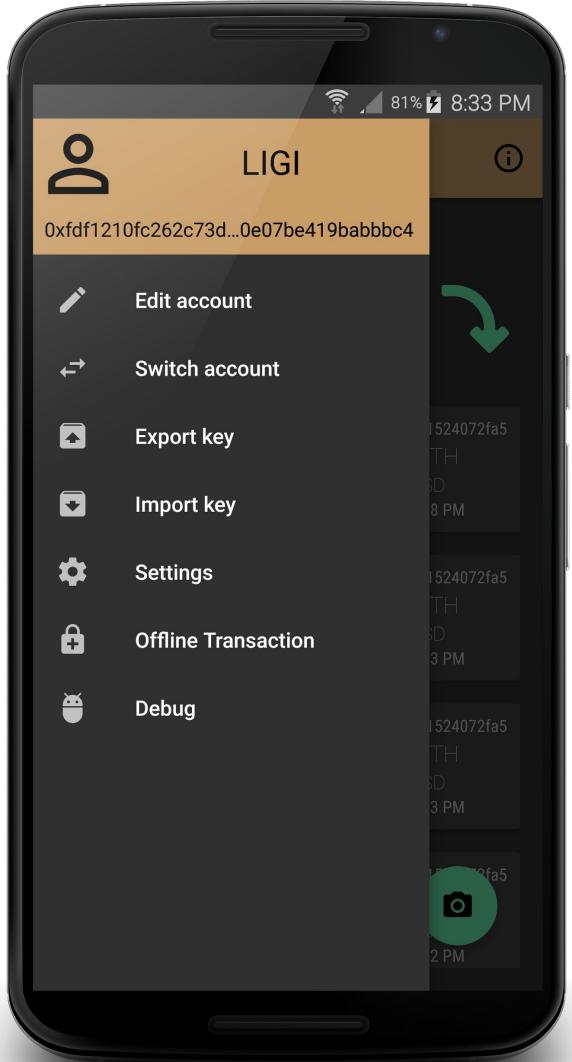
ERC-67

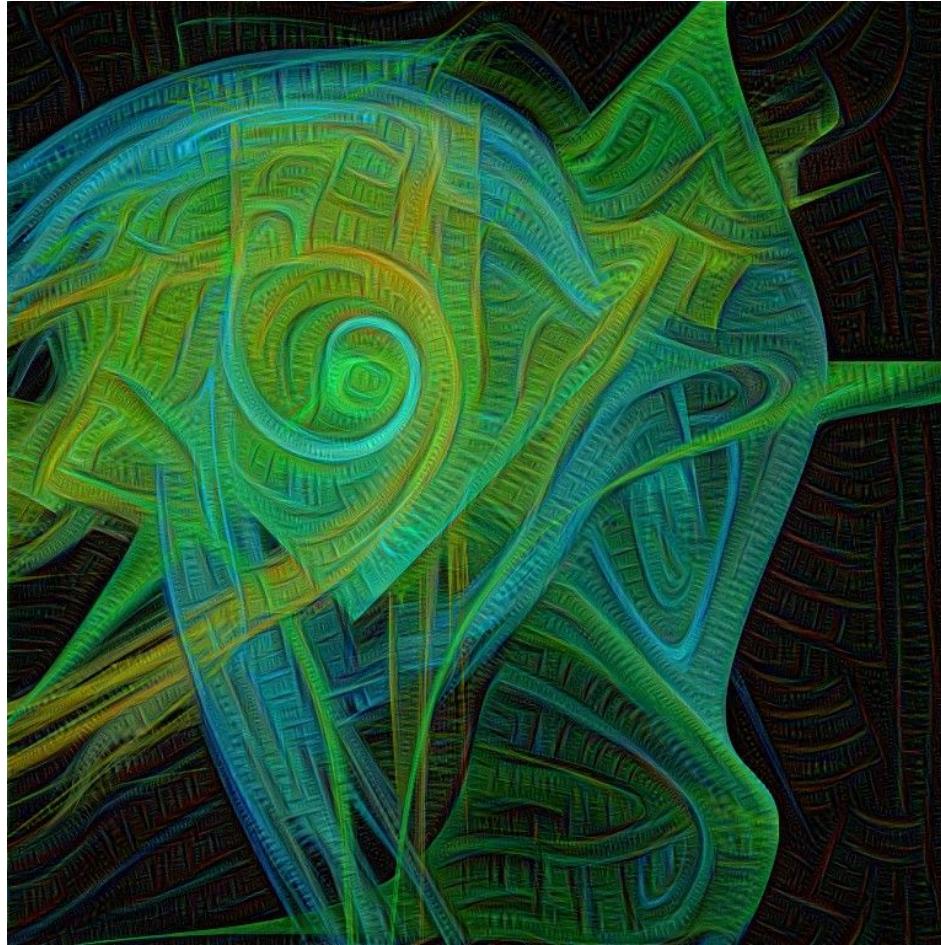
JSON / UTC- KEY

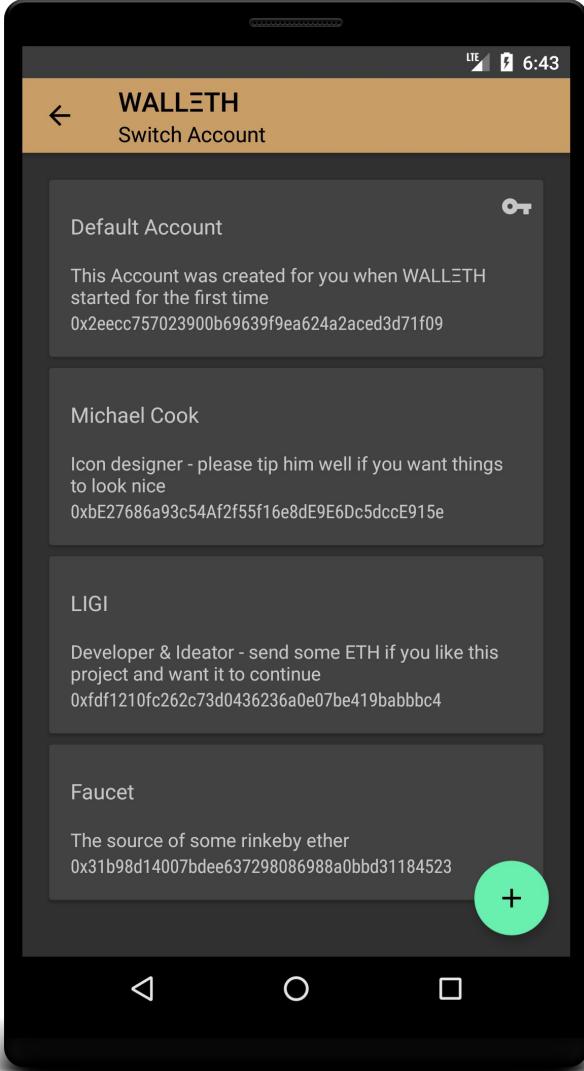
ECDSA raw KEY

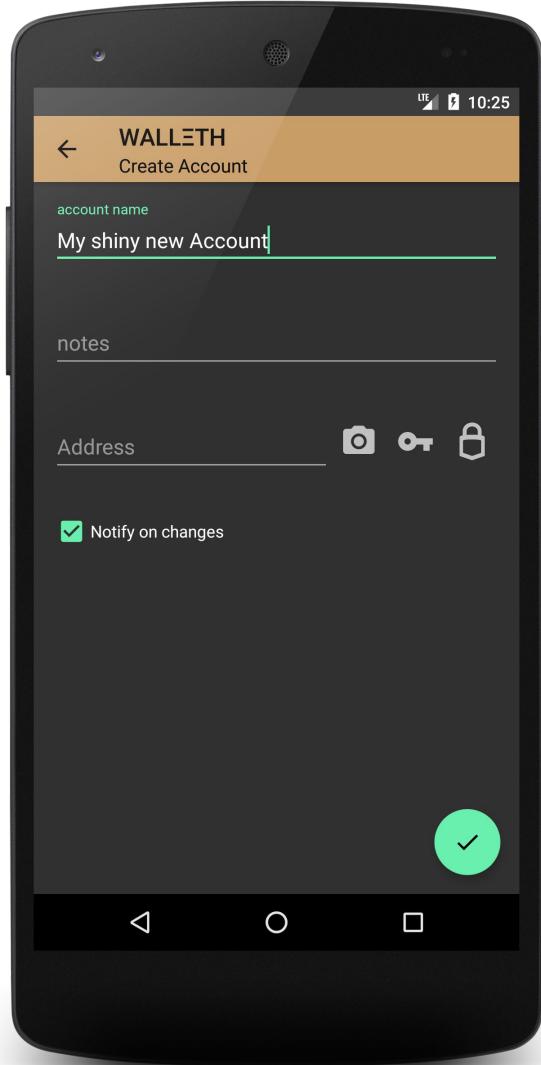
Address

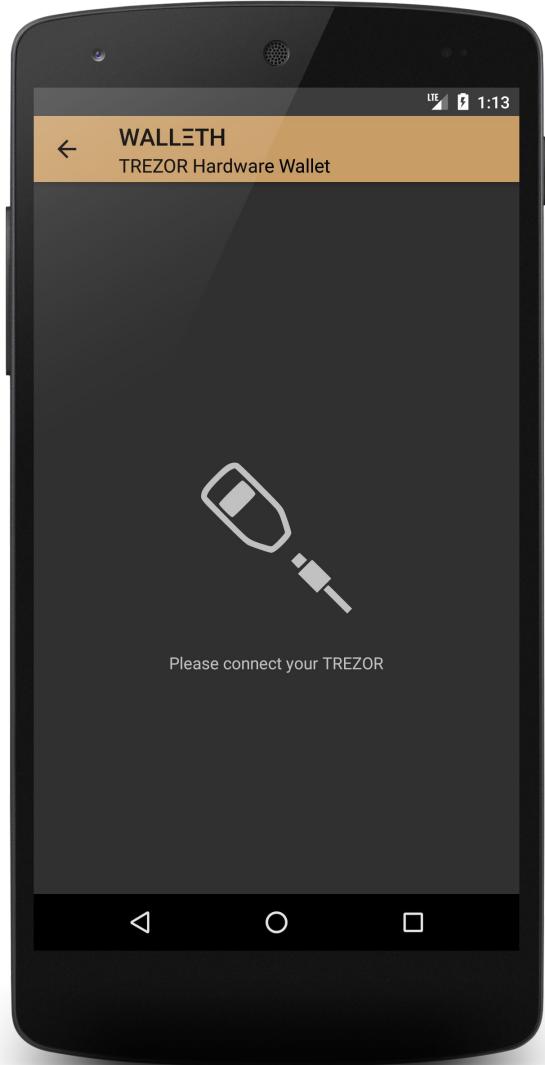
Missing: RLP for offline-transactions

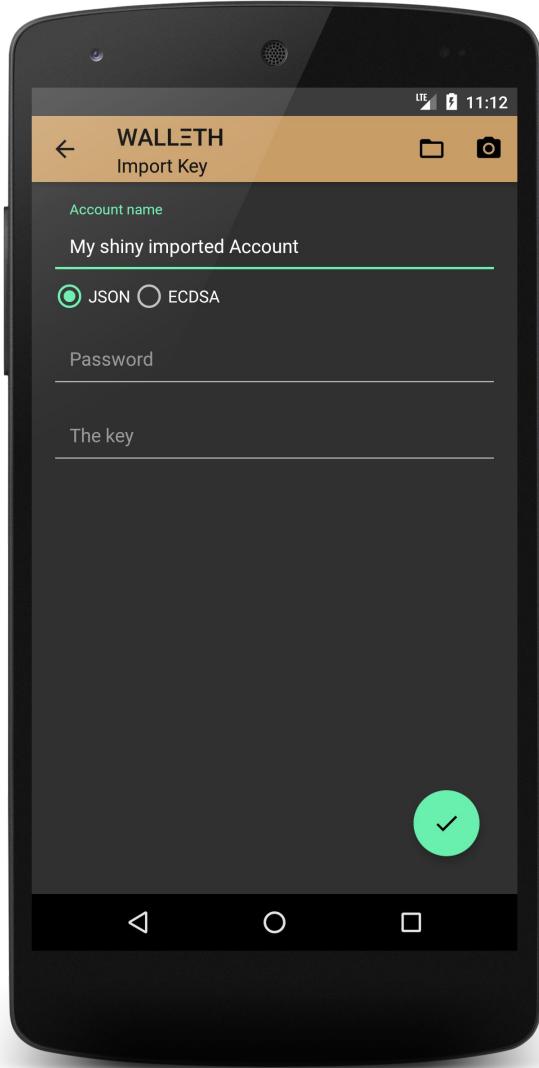


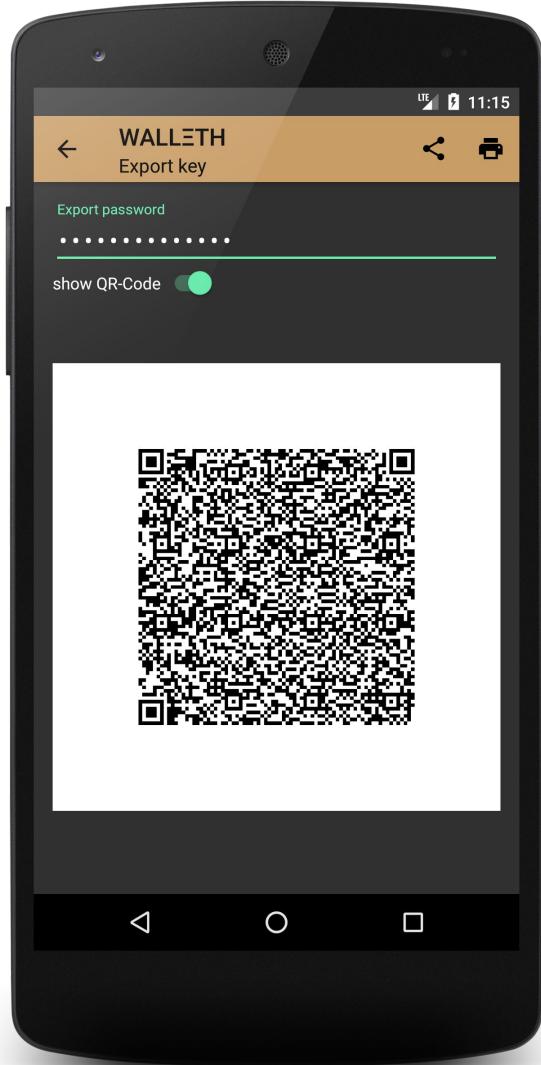


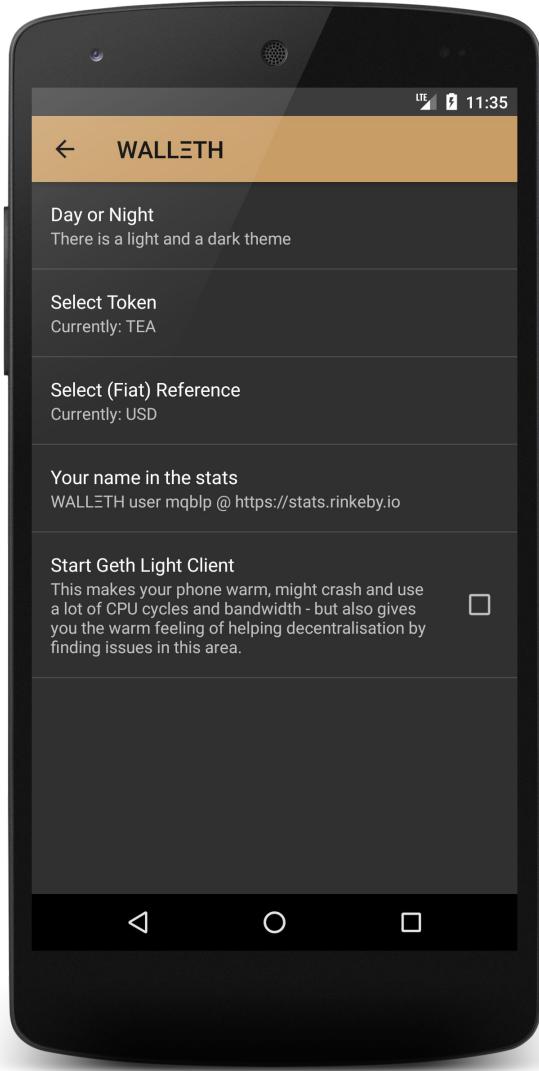


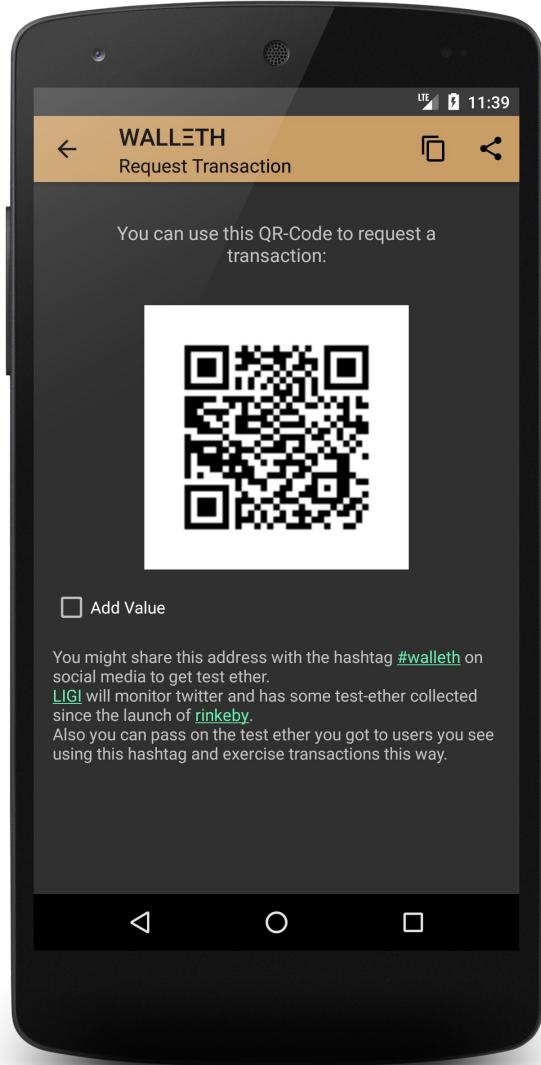






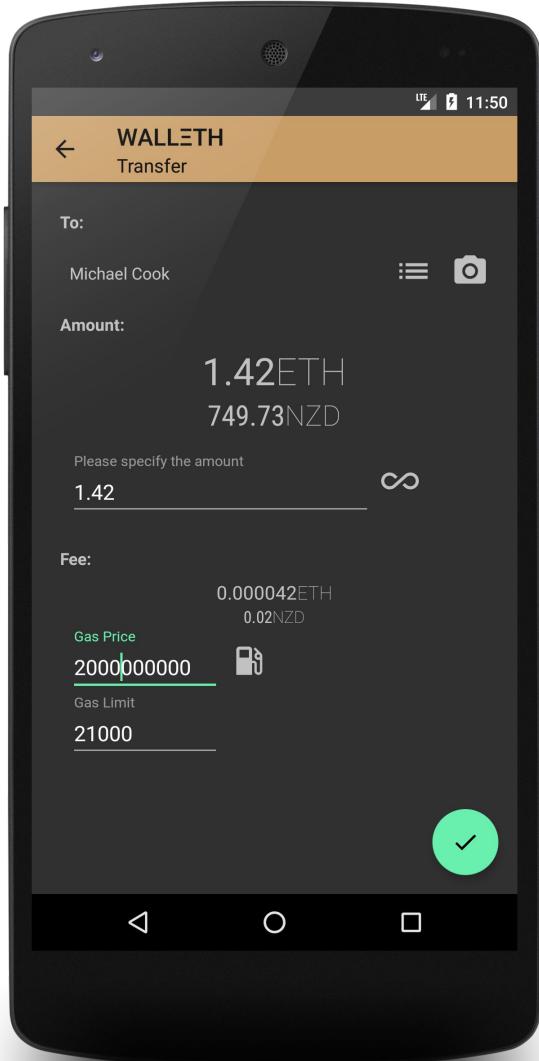








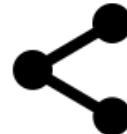




# Common symbols



Scan a code



Share



Offline transactions



Private Key



TREZOR Interaction



Copy content



**pw2**



# Developer

# 4 Fixed cornerstones:

- FOSS
- Native pure android
- Light client option
- Keys@User



**go-ethereum**  
**(geth)**



## ⌚ Invalid transaction v,r,s values with geth when reading from of signed MEW RLP transaction

#14599 by ligi was closed a day ago

## ⌚ mobile: Import raw key

#14481 by ligi was closed 21 days ago

## ⌚ wiki: broken link

#14457 by ligi was closed on May 13

## ⌚ Android API: expose the raw bytes of a transaction

#14443 by ligi was closed on May 11

## ⌚ Mobile: go.Seq\$Ref.finalize() timed out after 10 seconds

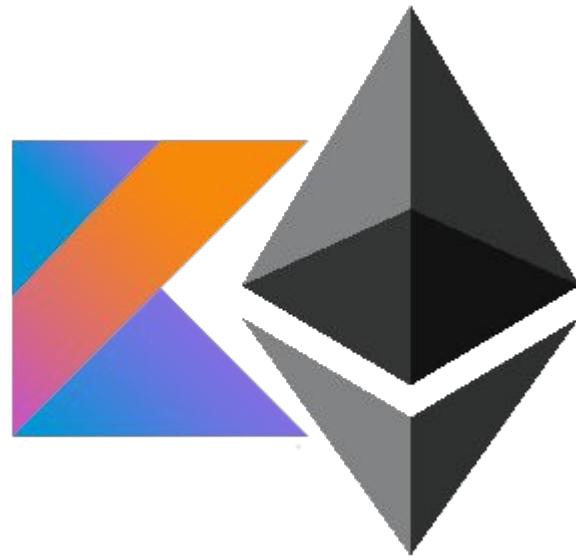
#14429 by ligi was closed on May 5

## ⌚ Mobile: fatal error: heapBitsForSpan: base out of range

#14422 by ligi was closed 22 days ago

## ⌚ fatal error: runtime.SetFinalizer: pointer not in allocated block

#3772 by ligi was closed on Mar 15





Dan Kim [Follow](#)

Android Programmer at Basecamp | <https://twitter.com/dankim>

Jun 10 · 2 min read

# Kotlin makes me a happier (better) programmer

What's Kotlin's best feature? Creating programmer happiness.





This organization

Search

Pull requests Issues Marketplace Gist



# WALLETH

The native Android Ethereum light client wallet



Earth



http://walleth.org

Repositories

People 1

Teams 0

Projects 0

Settings

## Pinned repositories

Customize pinned repositories

### ≡ walleth

native Android Ethereum light client wallet

● Kotlin ★ 26 3

### ≡ kethereum

Kotlin library for Ethereum

● Kotlin ★ 2

### ≡ walleth.github.com

Website / LandingPage

● CSS ★ 2

### ≡ walleth-push

Service that watches the ethereum network via RPC and triggers FCM pushes when registered addresses have new transactions.

● Kotlin ★ 1



Commits on Jun 14, 2017

-  **Bump version to 0.14**  
ligi committed 21 hours ago 

-  **Extract strings**  
ligi committed a day ago 

-  **Account -> Key**  
ligi committed a day ago

-  **Prevent negative result 1**  
ligi committed 3 days ago

-  **Initial offline transaction**  
ligi committed 4 days ago

### All checks have passed

5 successful checks

  kontinuum/assemble	— result	<a href="#">Details</a>
  kontinuum/checkout	— checkout done	<a href="#">Details</a>
  kontinuum/lint	— result	<a href="#">Details</a>
  kontinuum/spoon	— result	<a href="#">Details</a>

Verified



1a78c7b



Verified



cc23e78



Verified



44564af



Verified



68cc6e3



Verified



c24e145



Commits on Jun 13, 2017

-  **Ability to display RLP (signed/unsigned) as QR code for activity and...**  


Verified



f92b880

<https://gateway.ipfs.io/ipfs/QmRxrj8aifHjASVQqE8TskCpwuCNmq75MJxXaHkhn1XEQC>

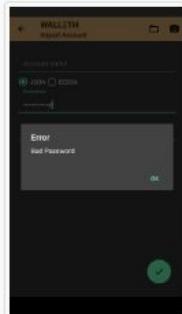
Saves Valid Address



When ,creating ,new ,address ,old ,gets ,cleared



Bad Password Is Rejected



Happy Path Works



ERC: Standard URIs ×

GitHub, Inc. [US] | <https://github.com/ethereum/EIPs/issues/67>

jbenet commented on Mar 20 • edited

+

Is this still the latest on achieving a QR code standard? We need to use a QR code for easier payments. We see some wallets have started doing QR codes, but are different from each other. What's holding this standard up? this should be pushed or we'll have a fragmented space that's frustrating to deal with (for products and users).

1	1
---	---

ERC: Standard URI [S](#) X ligi

GitHub, Inc. [US] | <https://github.com/ethereum/EIPs/issues/67>

ligi commented 20 days ago

+

4. Our existing QR codes are pretty raw - just address and just private key, no params. We hope to make one that users can easily scan in order to auto-fill a TX. Our private key QR codes will be updated to look different than TX/address ones.

Is there a consensus if ERC-67 is only intended for transactions or should it also cover other use-cases in the ethereum space. The private key you mentioned is one example. Another one would be RLP raw data to relay (e.g. from a hardware wallet). I think there will be many more use-cases in the future. Currently these barcodes are often plain - so the user has to know and add the context. Would love to see ERC-67 cover more use-cases so we can allow other flows. This is also important for intent-filters on android to e.g. allow just scanning a barcode without going in the correct app first.

ERC: Standard URI × Display address as | ligi

GitHub, Inc. [US] | https://github.com/MetaMask/metamask-plugin/issues/1479

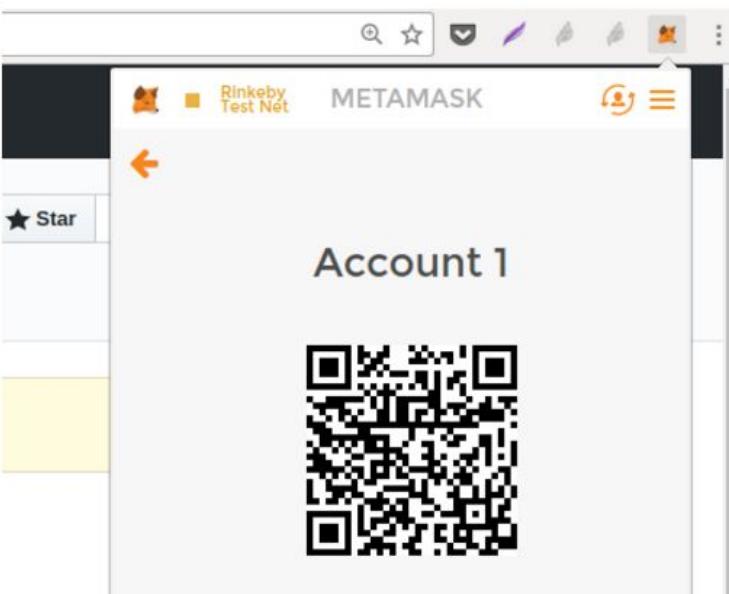
**Edit** **New issue**

# Display address as ERC-67 #1479

**Open** ligi opened this issue 22 days ago · 0 comments

ligi commented 22 days ago • edited

Currently when showing the barcode for the account metamask displays the raw hex string. But it would be good if context is supplied via e.g. ERC-67 ([ethereum/EIPs#67](#))



Assigees  
frankiebee

Labels  
L3-userinterface  
P3-soon  
T1-enhancement

Projects  
None yet

Milestone  
Core Maintenance

Notifications  
**Unsubscribe**

You're receiving notifications because you authored the thread.



ligi added a commit to ligi/k-9 that referenced this issue 17 days ago

↳ Add support for ethereum (ERC-67) URIs ...

Verified

bfcfcf7f



ligi referenced this issue in k9mail/k-9 17 days ago

**Add support for ethereum (ERC-67) URIs #2556**

Merged



ligi added a commit to ligi/k-9 that referenced this issue 17 days ago

↳ Add support for ethereum (ERC-67) URIs ...

Verified

44e2954



# Attacker



- ☐ ! **Address Cloak & Dagger attack** enhancement Security

#16 opened 18 days ago by ligi

---

- ☐ ! **TREZOR support** enhancement Security

#15 opened 20 days ago by prusnak

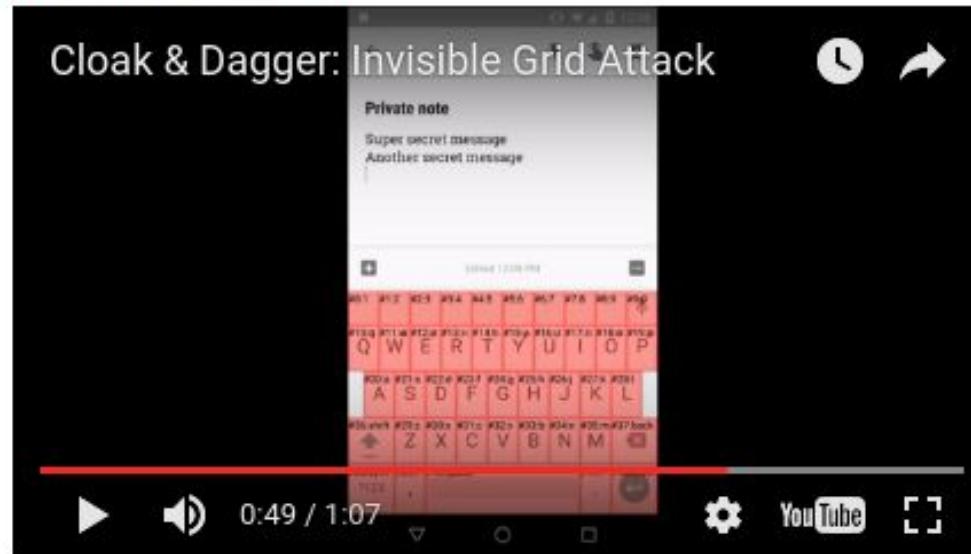
---

- ☐ ! **Address clipboard attack** enhancement Security

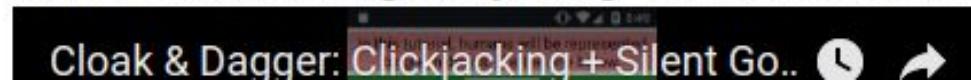
#14 opened 21 days ago by ligi

# Demos

## Invisible Grid Attack



## Context-aware/hiding Clickjacking + Silent God-mode Install Attack





# TREZOR

Pull Requests · trezor · GitHub

Filters ▾  is:pr author:ligi is:closed

Labels Milestones

New pull request

Clear current search query, filters, and sorts

0 Open ✓ 9 Closed

Author ▾ Labels ▾ Projects ▾ Milestones ▾ Reviews ▾ Assignee ▾ Sort ▾

Remove constraintlayout dependency ✓

#25 by ligi was merged 2 days ago

4

Use build-plugin 2.3.3 ✓

#24 by ligi was merged 3 days ago

1

Cleanup - remove unreferenced/dead XpubActivity and collateral ✓

#22 by ligi was merged 6 days ago

1

Add info on howto add library via jitpack - closes #1 ✓

#21 by ligi was merged 6 days ago

1

Add gradle witness build-plugin and library whitelists - closes #16 ✓

#20 by ligi was merged 6 days ago

4

Cleanup

#19 by ligi was merged 6 days ago

1

Replace JARs with maven dependencies for tagsoup and joda-time ✘

#17 by ligi was merged 16 days ago

8

Use kontinuum, care for lint-errors(\*) & Cleanup ✘

#14 by ligi was merged 16 days ago

1

Modernize (gradle 3.5, sdk/support 25) and DRY/Cleanup ✘

#13 by ligi was merged 16 days ago

1

[Code](#)[Issues 4](#)[Pull requests 0](#)[Projects 0](#)[Wiki](#)[Insights](#)[Filters](#) is:issue author:ligi[Labels](#)[Milestones](#)[New issue](#)[X Clear current search query, filters, and sorts](#)[0 Open](#)[✓ 4 Closed](#)[Author](#)[Labels](#)[Projects](#)[Milestones](#)[Assignee](#)[Sort](#)

### Add some Ethereum logos for homescreen

#23 by ligi was closed 4 days ago

 4

### Missing LICENSE

#18 by ligi was closed 16 days ago

 2

### Add gradle-witness

#16 by ligi was closed 6 days ago

 1

### Add to FDroid

#15 by ligi was closed 6 days ago

 6

# Signature:

- Old T42 (thanks js@c-base.org)
- Google signing?
- Split-apk?



# Offline Survival Manual

# WALL Tokens from now:

- 1 = talk attendance (with Android device)
- 3 = for first report of crashbug
- 42 = for one Unicorn token
- 5+ = for merged PR
- TBD

# WALL Tokens beta/release:

- 1 for 5 hand-smartphone-photos with installed WALLET
- 5+ for Translations (transifex\*)
- ?+ for support help



Wide-angle



<http://espass.it>





Your (D)APP?

# Look up an Ethereum Name

walleth

.eth

[UNWATCH](#)

TIME REMAINING UNTIL AUCTION  
ENDS

35h 5m 41s

2017-06-14 15:00

## walleth.eth waiting for bids to be revealed

After an auction ends its 72h period of bidding, all bidders have 48h to reveal their bids or forfeit their whole deposit. During this period, no new bids can be made. If no bids are revealed, the name can be requested again after this period ends.

### YOUR BIDS

You were willing to pay at most: **0.424242 ether** but since someone else was willing to pay more, your full deposit was returned, minus a bidding fee of **0.002121 ether** which was burned.

CURRENT HIGHEST BIDDER  
**0.69** ETHER

CURRENT SECOND-HIGHEST  
BIDDER  
**0.4242424242** ETHER

WATCHED NAMES

Wider context: Android go , Android Things



**URI ERC-XX**

**Password: XX**

**8WALL -> 1TEA**

# Big UP!

Go Team

Ethereum Foundation

MEW Team

TREZOR Team

Android Team

Jetbrains

EtherScan

CryptoCompare

Ryan Taylor

Michael Cook

Andreas Schildbach

Solidity Team

++

# Thanks for your Attention!

Follow-up

Project: [walleth.org](http://walleth.org)

Me: [ligi.de](http://ligi.de)



# Your lense (Q/A)

Follow-up

Project: [walleth.org](http://walleth.org)

Me: [ligi.de](http://ligi.de)