# Enhancements to the Desktop GUI Wallet for ZCash	# Grant Proposal

Document overview:

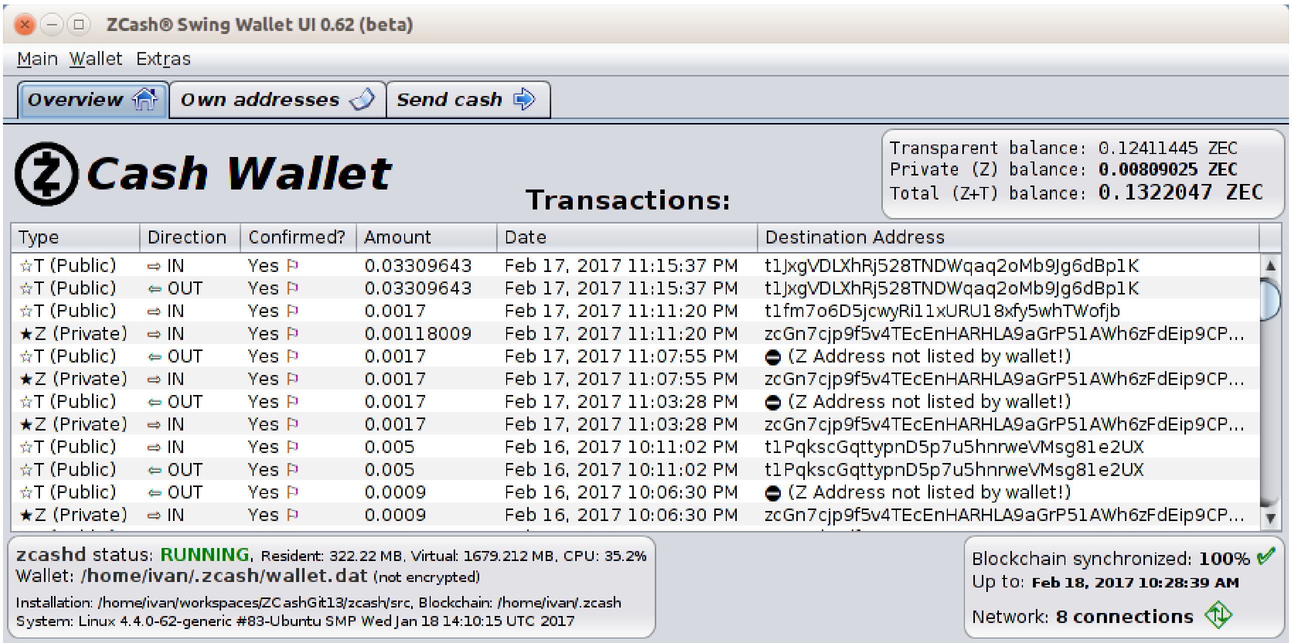
Brief Description:	Enhancements to the Desktop GUI Wallet for ZCash
Author:	Ivan Vaklinov
Project manager:	Eran Tromer
Date:	October 2017

History:

Date:	Name:	Description/Changes:
01.10.2017	Ivan Vaklinov	Created – described the concept, ideas etc.

1. Motivation and overview

I am the author of the Desktop GUI Wallet for ZCash:



Transactions:

```
Transparent balance: 0.12411445 ZEC
Private (Z) balance: 0.00809025 ZEC
Total (Z+T) balance: 0.1322047 ZEC
```

Type	Direction	Confirmed?	Amount	Date	Destination Address
☆T (Public)	⇨ IN	Yes ⚐	0.03309643	Feb 17, 2017 11:15:37 PM	t1JxgVDLXhRj528TNDWqaq2oMb9Jg6dBp1K
☆T (Public)	⇦ OUT	Yes ⚐	0.03309643	Feb 17, 2017 11:15:37 PM	t1JxgVDLXhRj528TNDWqaq2oMb9Jg6dBp1K
☆T (Public)	⇨ IN	Yes ⚐	0.0017	Feb 17, 2017 11:11:20 PM	t1fm7o6D5jcwyRi11xURU18xfy5whTWofjb
★Z (Private)	⇨ IN	Yes ⚐	0.00118009	Feb 17, 2017 11:11:20 PM	zcGn7cjp9f5v4TEcEnHARHLA9aGrP51AWh6zFdEip9CP...
☆T (Public)	⇦ OUT	Yes ⚐	0.0017	Feb 17, 2017 11:07:55 PM	⊖ (Z Address not listed by wallet!)
★Z (Private)	⇨ IN	Yes ⚐	0.0017	Feb 17, 2017 11:07:55 PM	zcGn7cjp9f5v4TEcEnHARHLA9aGrP51AWh6zFdEip9CP...
☆T (Public)	⇦ OUT	Yes ⚐	0.0017	Feb 17, 2017 11:03:28 PM	⊖ (Z Address not listed by wallet!)
★Z (Private)	⇨ IN	Yes ⚐	0.0017	Feb 17, 2017 11:03:28 PM	zcGn7cjp9f5v4TEcEnHARHLA9aGrP51AWh6zFdEip9CP...
☆T (Public)	⇨ IN	Yes ⚐	0.005	Feb 16, 2017 10:11:02 PM	t1PqkscGqttypnD5p7u5hnrweVMsg81e2UX
☆T (Public)	⇦ OUT	Yes ⚐	0.005	Feb 16, 2017 10:11:02 PM	t1PqkscGqttypnD5p7u5hnrweVMsg81e2UX
☆T (Public)	⇦ OUT	Yes ⚐	0.0009	Feb 16, 2017 10:06:30 PM	⊖ (Z Address not listed by wallet!)
★Z (Private)	⇨ IN	Yes ⚐	0.0009	Feb 16, 2017 10:06:30 PM	zcGn7cjp9f5v4TEcEnHARHLA9aGrP51AWh6zFdEip9CP...

zcashd status: **RUNNING**, Resident: 322.22 MB, Virtual: 1679.212 MB, CPU: 35.2%
Wallet: **/home/ivan/.zcash/wallet.dat** (not encrypted)
Installation: /home/ivan/workspaces/ZCashGit13/zcash/src, Blockchain: /home/ivan/.zcash
System: Linux 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017

Blockchain synchronized: **100%** ✓
Up to: **Feb 18, 2017 10:28:39 AM**
Network: **8 connections**

This wallet has had an important role in the ZCash community since ZCash release. It was the first wallet to support shielded transactions and I believe it is currently still "the best desktop wallet", that allows users to control their private keys. The wallet has also been included in distributions like https://zcash4win.com/ and has been forked many times for other uses (it is **open source under an MIT license**).

I made this wallet because I am excited about ZCash and wish to contribute to its future development. Since this is a hobby to me, having some funding will help a lot. If the wallet is enhanced, it will give users a better UI experience and contribute to the advancement of Zcash! In connection with the Zcash Foundation Grants Call for Proposals (Q4 2017) I wish to apply for a grant to continue work on the wallet and enhance it.

Material interest disclosure: In addition to the wallet for Zcash I have worked on wallets for other crypto-currencies that may be regarded as forks of Zcash inclusing HUSH and ZENCash. I have received donations and sometimes direct payments for this work. The GUI wallet has also been forked independently by other developers many times, to be used for other crypto-currencies including Komodo (https://supernet.org/en/products/komodo-swing-wallet) and BTCZ. It may be expected that any features implemented as a part of this grant request will be co-opted by others due to the open source nature of the software. I wish not to be restricted by this grant proposal when it comes to working on wallets for other crypto-currencies!

The desktop GUI wallet for ZCash that I have created, is in the same category as Bitcoin-QT with respect to user experience (but does not have as many features as Bitcoin-QT). It is not as easy to use as JAXX (which I would categorize as currently the most user-friendly ZCash wallet). Even after the implementation of the potential improvements I am proposing, the desktop GUI wallet ZCash will still be in the same category… However it will provide a better user experience. It will still be better suited to users who have some understanding of the basic concepts, such as the fact that there is a “blockchain” and that it needs to be “synchronized” etc. **I think the use of wallets incorporating a full node needs to be promoted since this generally strengthens the network.**

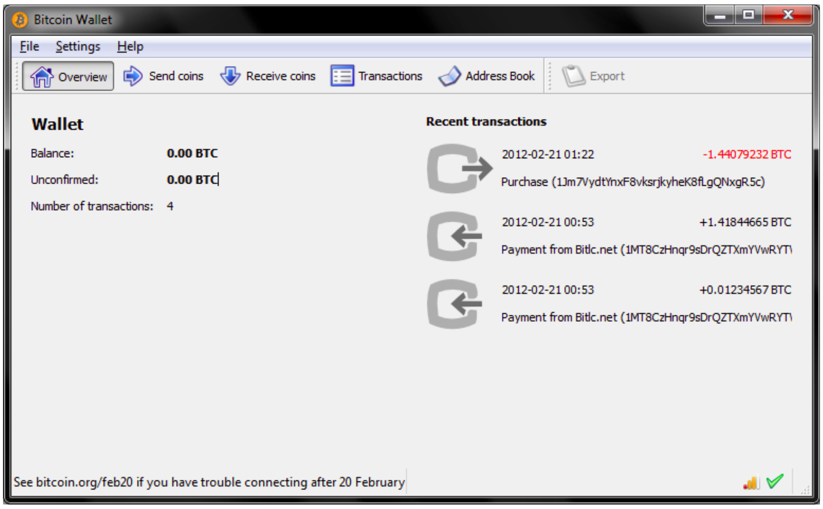
2. Technical approach

The specific enhancements for the wallet I have in mind are

- ➔ Improve the graphical appeal of the GUI (looks OK now but could be better): The full list of all transactions (GUI table) goes to its own UI TAB. The first TAB (overview) gets a complete overhaul: the T/Z balance is displayed prominently and more beautifully. The last 4-5 transactions (only) are shown in the overview tab with full details. The detail panels about blockchain, zcashd etc. are to be changed: each panel must use more graphice/icons and by default show just some basic info (e.g. green icon for a synchronized blockchain). The user may click a button of type “expand” to show the full contents of the respective panel with the kind of detailed information shown now. A toolbar is to be introduced with the most important actions.
- ➔ Usability enhancements like regularly reminding users to backup their wallet.dat, to keep it safe on another system/backup medium etc. The wallet will remember when users made their last backup and advise users to make a new backup…
- ➔ The “Send cash” TAB should allow users to sweep small change (or not small - balance) from multiple addresses (will work with T addresses only) and send cash to multiple addresses (T or Z) at the same time. This is useful to miners and often requested (such as for sending from multiple taddrs at once to a taddr)
- ➔ An extension of the “Send cash” TAB will allow users to make donations, to the developer(s) of the wallet (i.e. me) or to other non-profit entities designated by the ZCash foundation. Users will be able to make donations straight from the wallet.
- ➔ The current version of the wallet also allows users to send a message in the encrypted memo field of shielded transactions. Enhancements could be made in the visualization of incoming memos (for user convenience) - friendlier memo send/receive interface.
- ➔ Multiple proving key download URL support (including manual input) – upon downloading the proving key, the user may choose from a list of URLs where to download the proving key from, or he may use a custom URL.
- ➔ Support for localization into different languages (low priority but could be included)

The risk to implementing all this is low - the wallet already exists and is functional. It just needs enhancements and maintenance.

After the completion of the work the Desktop GUI Wallet for Zcash will be in some ways similar to Bitcoin QT but will be a little more graphically appealing (than this):



Wallet

Balance: 0.00 BTC

Unconfirmed: 0.00 BTC

Number of transactions: 4

Recent transactions

2012-02-21 01:22 -1.44079232 BTC
Purchase (1Jm7VydtYnxF8vksrjkyheK8fLgQNxgR5c)

2012-02-21 00:53 +1.41844665 BTC
Payment from Bitlc.net (1MT8CzHnqr9sDrQZTXmYVwRYT\

2012-02-21 00:53 +0.01234567 BTC
Payment from Bitlc.net (1MT8CzHnqr9sDrQZTXmYVwRYT\

See bitcoin.org/feb20 if you have trouble connecting after 20 February

@radix42 and I have cooperated before and I am sure we can do it again. Once the features of this grant proposal are implemented, they will be merged in the distributions of http://zcash4win.com/ and https://zcash4mac.com/...

---

3. Team background and qualifications

I am a one-man-team more or less (with respect to this project), and I am a professional developer. Developing this wallet is a hobby to me. I believe I have already proved my qualifications to do the work ;-) Apart from this I have been working as a developer for 18 years in the product area of B2B integration middle-ware using standard and enterprise Java technologies. I have a masters degree as a “computer systems engineer” - awarded in 2001.

---

4. Evaluation plan

Once the features are implemented (at each stage/feature), they may be evaluated by the Grant Review Committee and/or other community members. All wallet features will be published in the wallet GitHub repository and be immediately testable/usable. The measure of success will be satisfied ZCash wallet users (having good UI experience). The progress of the implementation may be followed and partly quantified by noting what percentage of the features in the list have been implemented. I would be willing to make monthly progress reports...

---

5. Security considerations

This project promotes good security practices in the community. It encourages users to run a full ZCash node on their desktop computer and to control their private keys locally – which mean greater privacy to users. It also has functionality allowing users to back up their wallets.dat etc. The use of such wallets makes users (generally) less vulnerable – unlike the use of “server wallets” that control user’s private keys and exchanges.

If this kind of wallet remains popular (by some current estimates 40% of users have it) it will have a significant contribution to the decentralization of the Zcash network. It will make it easier to avoid a trend similar to Bitcoin’s where the network has become ever more “centralized”.

---

6. Schedule

The 6-7 proposed features will take me perhaps 4-5 months since I do this as a hobby. Each feature will be pushed to GitHub and be usable separately. Some verifiable results will be available within the first 1-2 months. It will be possible to evaluate each specific feature as it gets completed. I hope and expect to be able to start this project in early December 2017.

One example (expected) time-line is:

- ➔ 15 Dec 2017 – start of project work
- ➔ 1 Feb 2018 – completion of feature “Improve the graphical appeal of the GUI...”
- ➔ 15 Feb 2018 – completion of feature “Usability enhancements like regularly reminding users to backup their wallet.dat … “
- ➔ 1 Mar 2018 – completion of feature “The “Send cash” TAB should allow users to send from multiple addresses and to multiple addresses”
- ➔ 15 Mar 2018 – completion of feature “An extension of the “Send cash” TAB will allow users to make donations”
- ➔ 1 Apr 2018 – completion of feature “Friendlier memo send/receive interface.”
- ➔ 10 Apr 2018 – completion of feature “Multiple proving key download URL support”
- ➔ 30 Apr 2018 – completion of feature “Support for localization into different languages (low priority but could be included)”

---

7. Budget and justification

I have asked for donations to fund my development effort on this project, but as can be seen in the donation address:

https://explorer.zcha.in/accounts/t1UMGjLDipdfuCdNwxUZTV4FhM34FJXgM8r

the amounts donated so far have been minimal and my only motivation to move forward with it has been non-financial. I would estimate my development effort (wallet GUI work) on the above proposed features to be worth approx. **4500 USD** if evaluated on the basis of "work done for hire". Of course I have spent a great deal of effort on the wallet so far that has not been paid... This project is flexible and more or less work/features may be implemented based on the funding received. No new equipment or external services need to be purchased for this project to proceed. Like before, I shall use my home computers to implement it.

This grant proposal will cover all UI development in the wallet software per se. I am prepared to collaborate with anyone on this who is willing to do a part of this "UI development". Once sizeable parts of this UI developemnt are ready we shall collaborate with @radix42 to merge them into his code base for release to the community (we have done this before on e.g. https://zcash4win.com/).

Important: I have not made any arrangements for splitting the budget. If anyone expects to get a part of the budget of this proposal, we need to make arrangements before start (who will implement which parts for what share etc.) If this is not done at start, it may become a point of disagreement later. @IDEO-coLAB have offered to collaborate on the GUI with expert advice. I would welcome such collaboration but it needs to be budgeted separately.