The application for Zcash foundation grant 2017Q4

Stage I Android wallet

October 05, 2017
Tallinn, Estonia

Table of content

TABLE OF CONTENT 2

MOTIVATION AND OVERVIEW 3

TECHNICAL APPROACH 3

In general the wallet consists of the following parts: **4**

High level architecture can be described as follows: **4**

Network HL architecture: **5**

Zcash Shielded transactions **6**

TEAM BACKGROUND AND QUALIFICATIONS 6

EVALUATION PLAN 7

SECURITY CONSIDERATIONS 7

SCHEDULE 7

BUDGET AND JUSTIFICATION 8

Motivation and overview

We are a group of blockchain enthusiasts with background in software development, and product management. We have a distributed team from EU, Russia and Ukraine. At the moment we have experts from IT, FinTech, Blockchain, Security, Marketing, Design, UI/UE.
Recently we have united together to develop a project called Guarda. Mobile cryptocurrency wallet which would make using any cryptocurrency easy, accessible and secure.
Our wallet for the first currency was launched in September 2017 on Google Play.
Zcash is one of our favorite blockchains thanks to technological supremacy, great development team and clear value proposition. As a team of crypto enthusiasts we believe in anonymity as key feature of decentralized currencies and blockchain technology overall. Zcash already is in our development roadmap. However development of Zcash light wallet is yet an issue due to the lack of open source mobile light wallet implementations.

Technical approach

We are guided by several core principles:

- Building trustless solutions.
  If customer wants to rely on other blockchain node he\she can type in this information.

- Multicurrency approach.
  We thoroughly choose best cryptocurrencies and willing to support them all.

- Respect customers privacy.
  We do not require any KYC or customers data. No registration is required as well.

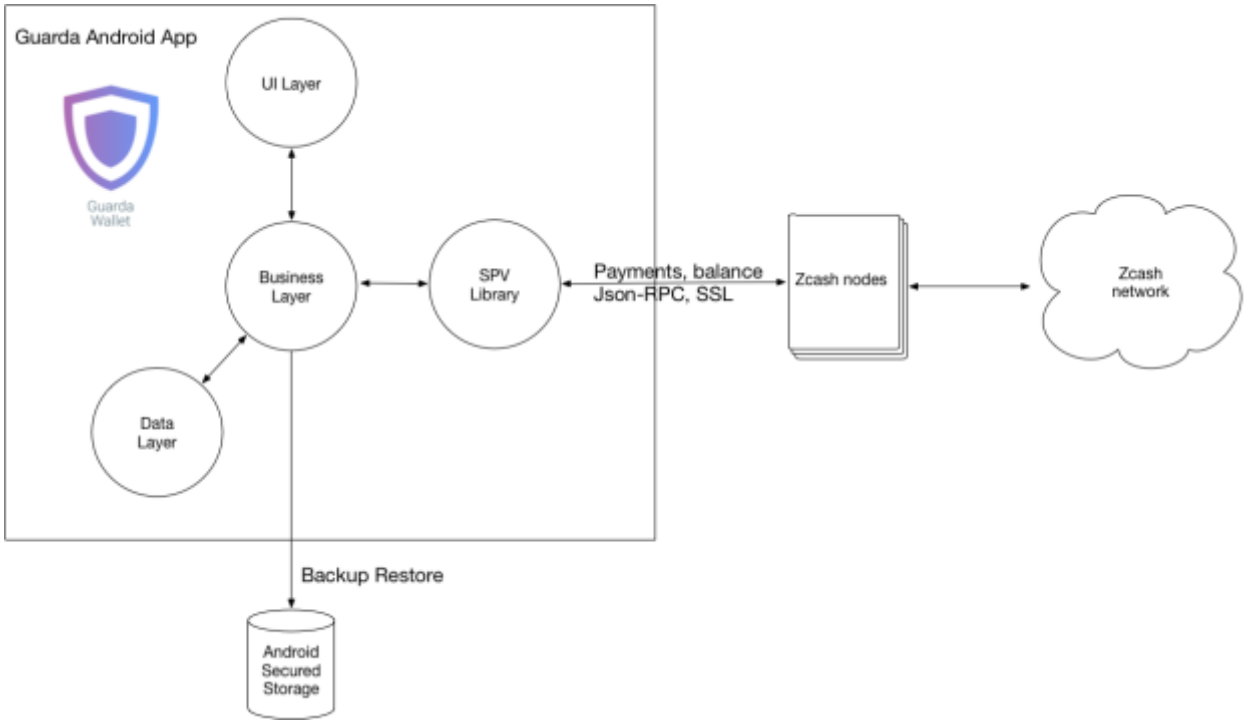
- Never touch customers funds.
  The proposed wallet is a light wallet allowing customer manage his\her keys himself.

- Never touch fiat.
  Purchase of cryptocurrencies will be delivered in collaboration with professional payment gateways.

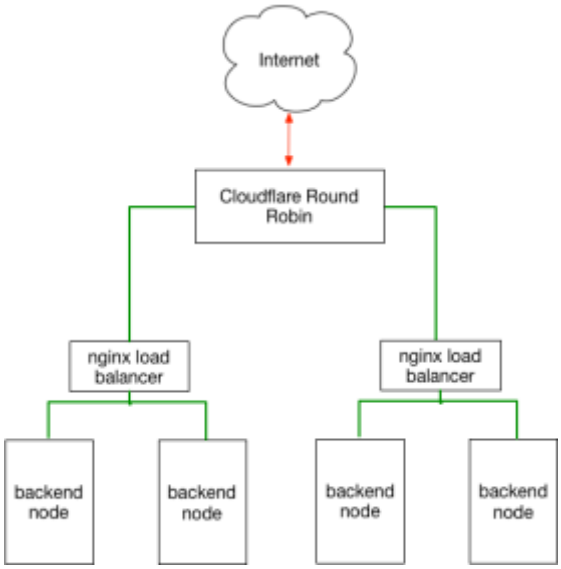
In general the wallet consists of the following parts:

- Server side node
  Blockchain community developed solution. Open-source and distributed free.
- Lightwallet (SPV) library
  This allows you to work with the cryptocurrency blockchain, without the additional overhead of having to write your own integration code for the platform. Usually the library interacts with the server side node through JSON RPC. As we are applying for a grant we believe this part of our work should be open sourced and available for public on a royalty free basis.
- GUI layer integration
  Customer experience oriented graphic user interface running Android of the mobile phone.

High level architecture can be described as follows:



Network HL architecture:



We have three basic stages for the wallet implementation:

- Everything starts from the own blockchain nodes deployment. We have own primary and backup nodes for the wallet support. In addition, we offer a range of third party nodes that can be applied by user. We are using sophisticated proxy for the node balancing in order to get up-to-dated blockchain status.
- The next step is mobile client library implementation. It is used by mobile wallet to manage transactions and abstract blockchain, security, cryptography layer from GUI developers.
- The last stage is the design implementation of mobile application. We are thriving to use trendy and cozy interfaces in our wallets to provide best customer experience.

We are developing light wallet which means that user private keys are always under the user control. The private keys are always on the customer device and managed only by user. The wallet signing a transaction on the device side and transmit the signed transaction over Internet using ssl to blockchain node.
The Guarda wallet implemented functions are:

- send coins
- receive coins
- exchange cryptocurrencies to zcash
- passcode app protection

To be implemented in following one and a half months (before Zcash wallet to be released):

- purchase Zcash for the fiat
  our committed partners for card transactions and SEPA payments are available to be disclosed upon request from Grant Review Committee.
- other node usage

- mnemonic phrase
- password encrypted keyfile

Zcash Shielded transactions

The shielded transactions will be supported by Guarda wallet along with transparent ones. The shielded transaction can occupy device resources or lead to system crash. Within the project we will be looking for a suitable UE solution in order to fulfill the customer's expectations. In the short term, we're considering to use one of the following approaches:

1. The shielded transactions are available for all devices. It sounds like a doubtful idea, some devices probably can be stucked, anyway we need to check it. We're going to perform the test/benchmarking how it will work in order to evaluate this approach.
2. The shielded transactions will be available for the powerful devices only. We'll rate the devices based on it's hardware. The shielded transactions will be available only for the high-rated devices with suitable transaction calculation time.
3. Spreading the calculations between the customer device and guarda server. We'll use a secure way to communicate with server to keep the privacy.

We'll choose one of the mentioned above approaches (or tune it within latest zcash available tools) based on R&D results. It should meet our expectations for reasonable shielded transactions implementation.

Team background and qualifications

- Paul S., CEO, has three years experience in blockchain, 10 years in fintech. Certified banking cards security and business expert. Launched over 6 successful projects within last three years. Paul interests are: cryptocurrency exchanges, wallets, smart contracts, oracles.
- Ilia B., CTO, expert in blockchain, security and highload. Has 6+ years of experience in highload projects' development, 4+ years of experience in blockchain development. Designed and launched cryptocurrency billing system this year.
- Ondrej H., product manager, has 15+ experience in IT product management. Has in the portfolio projects from mobile ads, SaaS enterprise solutions, high load IT solutions, mobile app development and production.
- Vlad A., senior Android developer, 7+ years of mobile development
- Valentin S., senior Android developer, 6+ years of mobile development
- Alex N., senior iOS developer, 6+ years of mobile development
- Roman L., senior backend developer, expert in blockchain, has 3+ years of experience for blockchain development, cryptocurrency mining, etc.

Evaluation plan

We have quite tiny and reasonable schedule for the wallet implementation. The distributed team with a wide range of professionals gives us ability to launch in the parallel main project phases: shielded transactions implementation, mobile library and wallet GUI development.
We are using agile approach with continuous delivery, which allows us to present our progress and performance to the Grant Review Committee at any point in time.

Security considerations

Security is our priority. The light wallet approach itself is our vision for the secured blockchain wallet. The customer private keys are the most important and sensitive aspect.
We store keys in OS secure storage in an encrypted form.
We are using additional product features to increase the product resistance for the attacks. The team has already implemented PIN-code for the wallet access, password keyfile encyption is expected by the middle of October.
At the node side we are using network security tools, like a WAF with ML.

Schedule

In terms of limited grant budget, we suggest to split the project for two stages: development of Android wallet & development of iOS wallet. We estimate duration of "Stage I Android Wallet" as 11 weeks, and "Stage II iOS wallet" as 10 weeks:

week	**Stage I Android wallet**	**Stage II iOS wallet**
1	Hosting & node setup, UE	-
2	Node proxy, setup net security tools, android SVP library, UI mock ups	iOS SVP library, UI mock ups
3	Android SVP library development, UI prototyping	iOS SVP library development, UI prototyping
4	Android SVP library development, UI design	iOS SVP library development, UI design
5	Android SVP library development, android app implementation, UI design	iOS SVP library development, mobile app implementation, UI design
6	Integration with third parties services, android app implementation	iOS app implementation
7	Android app implementation	iOS app implementation
8	Alfa release android app, QA, bug fixes, mobile app implementation	Alfa release iOS app, QA, bug fixes, mobile app implementation

9	QA, bug fixes, beta-release, shielded transactions research	QA, bug fixes, beta-release, shielded transactions research
10-11	Project Risks worked	Project Risks worked

Budget and justification

We have estimated preliminary costs for the whole project for 60K USD. In order to reduce the financial load, we suggest to split the project for two stages – Android & iOS.

Guarda team wants to apply for the zcash Q42017 grant with Stage I Android wallet proposal. We have estimated preliminary costs for Stage I Android wallet for 30K USD that will cover almost all Stage I issues.

The Stage II iOS wallet will be proposed as separate application within for the following grant program.