Rune

PKT Cash - Network Steward Proposal

February 29th, 2020

Project Synopsis

Project Name: ***Rune Blind-Trust Transaction Engine & Wallet***

Contact Email: ***LinFisher@mac.com***

Project participants: ***Michael "Mehow" Pospieszalski (***mehowfnm@me.com***)***

Justus Ranvier (Justus@opentransactions.org***)***

Lin Fisher (linfisher@mac.com***)***

Projected duration: ***4 SPRINTS over 4 to 5 months***

Projected effort: ***5.5 people full time for 4 to 5 months***

Requested PKT contribution: ***Request: 39m PKT for first 3 milestones***

PKT address to pay to: e.g. ***pGLkefsW74NAHCHBDfM9cNGrEJSc7k7AJq***

Project status: ***PROPOSED***

Project Deliverables

The project will be creating new software and will us "All MPL-2" licensing.

New Software - GUI and Command Wallet App Using for Desktop and Mobile

https://github.com/FellowTraveler/opentxs.

The software will be hosted in:

https://github.com/FellowTraveler/opentxs.

The maintainer of this software will be: Justus Ranvier and Michal "Mehow" Pospieszalski. Our Chief Architect responsible for managing the open source project will be Justus Ranvier. Justus is the inventor of BIP-47 and Chief Architect of Open Transactions.

JUSTUS **RANVIER**

+1 (512) 348-8576
justus@opentransactions.org
github.com/Open-Transactions/opentxs

Experienced protocol designer and C++ architect/developer, with expertise in crypto and blockchain, seeks on-site or remote position in Austin, Charlotte, LA, SF or NYC.
Lead Developer of the Open-Transactions financial crypto library in C++.

Developed several blockchain-related protocols for secure custody and ease-of-use of cryptographic tokens. Recognized cryptocurrency expert in the blockchain industry. Familiar with modern C++ standards and development practices (C++11 through C++17).

Productive/expert in hands-on coding, blockchain/crypto, remote work and on-site management.

EXPERIENCE

MAR 2019 - PRESENT
CHIEF SOFTWARE OFFICER, RUNE WALLET

A venture to bake Open-Transactions onto a smart card chip. Underfunded.
Recently acquired Stash for stock.

AUG 2015 - PRESENT
LEAD DEVELOPER, OPEN-TRANSACTIONS PROJECT

A cross-platform financial crypto library in C++ for on-and-off blockchain applications. All transactions are based on cryptographic proofs.

AUG 2015 – MAR 2019
LEAD ARCHITECT, STASH CRYPTO

A venture to build products integrating Open-Transactions with blockchain-based currencies, including a software wallet and a personal transaction server. Acquired by Rune.

APR 2014 – AUG 2015
LEAD ARCHITECT, MONETAS AG

Mobile payments system for Africa, including iOS and Android apps.

JAN 2010 – MAR 2013
STUDENT, UNIVERSITY OF TEXAS AT ARLINGTON

Electrical engineering program.

JUN 2006 – DEC 2010
INDUSTRIAL ENGINEER, TRINITY INDUSTRIES

Developed and maintained automated welding and manufacturing equipment.

JUN 1998 – JUN 2006
NUCLEAR REACTOR OPERATOR, US NAVY

Operated and maintained submarine nuclear reactor safety control systems.

Michal "Mehow" Pospieszalski
Cryptocurrency Expert, Serial Entrepreneur

Experience

Director, Blockchain Technologies
Exemplar Companies, Inc.
Mar 2018 – Present · 2 yrs
Greater Los Angeles Area

At Exemplar Companies we work with revolutionaries and game changers on capital, law, tax, and accounting. Fully FINRA and SEC licensed. We're a leading edge crypto fintech company in domestic utility, coin, and equity ICO/STOs, OTC cryptocurrency trading, and tokenized equity exchange! Accelerating and funding next generation crypto tech is my focus.


Chris Marston, CEO of Exemplar and myself at...


Nassim Haramein!

President, Co-founder
Rune Wallet
Jan 2018 – Present · 2 yrs 2 mos
Austin, Texas Area

Revolutionary off chain and on chain hardware and software wallets and servers. A Rune Wallet can transfer any cryptocurrency off chain but with the same level of security and end user autonomy as on chain. Access the world's best stable-coin, distributed exchanges that prevent fraud and theft, and BIP47 identity functionality and way more right in the wallet. We're making crypto as ...see more

CEO
Mehow Publishing, Inc.
Jul 2006 – Present · 13 yrs 8 mos
Los Angeles

Since 2006, Mehow has devoted himself to mastering the art of creating fulfilling relationships. Mehow has written eight books about attraction, dating and relationships. He has given countless talks and personally taught thousands of students and reached over 500,000+ consumers with his products and is responsible for countless relationships and marriages.. He is the host anc ...see more

Chief Technology Officer
Election Science Institute
Jan 2005 – Jun 2006 · 1 yr 6 mos
San Francisco Bay Area

Worked with the team to guide voting machine public policy based on my voting machine white hat analysis work.

Hacker, Chief Technology Officer
Various Government and Private Entities
Jun 1995 – Jun 2006 · 11 yrs 1 mo
Washington D.C. Metro Area

Mehow passed 70+ certification exams resulting in 20+ IT and programming certifications from Sun, Novell, Microsoft, Oracle, and Cisco. He's proficient ins C, C++, assembly, Java, Python, and everything web and network. Mehow has been programming since age 15. Initially focusing on network infrastructure creation he then moved on to network security and software secur ...see more

Success Criteria

The Network Steward should evaluate the success or failure of the Rune project by

- Users will be able to access balances and transfer PKT on chain to other users and transfer it to OT (Open Transaction) notaries using standard receive addresses and BIP-47 via command line and UI.
- All functional requirements will operate as proposed and within required parameters

For the purposes of this proposal, we have directly addressed each line item in the project's requirements outlined below. The excerpts and page references below refer to Rune Wallet's white-paper: "A Comprehensive Solution for Transactions of Blockchain-based Funds.

Team PKT / OT Wallet – comprising of Michal "Mehow" Pospieszalski, Justus Ranvier (Inventor of BIP 47), and Lin Fisher are proposing a open source version of the Rune/ Open Transactions wallet that supports and extends the desired PKT features.

For clarity we are elucidating how each feature will merge in with our existing crypto wallet. Existing wallet code is available for inspection at https://github.com/FellowTraveler/opentxs.

The following are bullets directly from the NS project list

- ***Checking the authenticity of the blockchain by verifying the PacketCrypt proofs on a configurable number of the most recent blocks and verifying only the connectedness of all earlier headers***
    - We already have begun coding our own BitCoin wallet that doesn't require a dedicated node to function. As such, all the blockchain verification checks are performed on the client device. Therefore, the above requirement would be met by adding additional methods to the existing client-side verification scheme.
- ***Ability to issue, transfer and validate colored coins***
    - We are coding SLP support presently.
- ***Ability to validate a message as signed by the current holder of a given colored coin***
    - This is already done in our messaging system.
- ***Ability to offer a colored coin for sale in a swap and ability to take such a swap transaction and accept it***
    - Swaps are currently supported natively in Open Transactions.
- ***Future interoperability with Lightning Network***
    - We're supporting BTC and BCH in its entirety.
- ***Compatibility with Android, iOS, Linux, OSX, Windows***

    - Rune/OT Wallet currently compiles on all those platforms.

- ***Graphical, command line and library modes***
    - Native to existing wallet.

- ***Low resource footprint***
    - We're using on-client filters that don't require a node for blockchain queries. We believe this is as lightweight as possible without offloading work to external machines which will compromise privacy.
    - Additionally – the wallet already supports BIP47 identity and traditional legacy receiving addresses. BIP47 allows for KYC/AML and send/receive of funds w/o having to generate receiving addresses:

> "The BIP-47 Payment Code is a way to format blockchain addresses so that each user can have a single, re-usable address across all blockchains, without the address itself appearing in any on-blockchain transactions, and thus cannot be observed publicly on-blockchain by any third parties, unless they have the party's private key. Instead, the receiving addresses are calculated deterministically via "spooky action at a distance" using a Diffie-Hellman shared secret. This is a process whereby each party, using his/her own private key and the other party's public key, is able to calculate a shared secret key, which no one else can calculate without one of the private keys. The parties also increment an index after each transfer, so there is a new blockchain receiving address calculated for each transaction between them."
>
> Furthermore, the wallet already supports Open Transactions such that the wallet can store funds on an off-chain Notary and perform instantaneous transactions on Notaries of the user's choosing.
>
> "The Open-Transactions (OT) project is a collaborative effort to develop a robust, commercial grade, fully-featured, free-software toolkit that implements off-blockchain transactions purely as cryptographic proofs."
>
> We define an off-blockchain transaction as a group of operations on contracts capable of objectively proving balances (and changes of balance) between adversarial parties. All transactions use the same basic structure: the parties involved sign agreements which, are then countersigned by an independent notary server. Transactions are irreversible since the receipts are always formed and signed on the client side first, before being notarized by any server.
>
> This prevents the notary from falsifying receipts since it can't forge the client's signature. This basic structure can be built upon

to create many types of financial instruments. Those supported by Open-Transactions include:

> **Transfers**. An atomic movement of funds from one account to a different account, similar to a bank account-to-account transfer.
>
> **Cash**. Untraceable cryptographic tokens which can be securely redeemed by the recipient without revealing the sender
>
> **Cheque**. A payment that is not deducted from the sender's account until the recipient claims it.
>
> **Voucher**. A payment that is deducted from the sender's account at the time of creation.
>
> **Invoice**. A payment request which the recipient can opt to pay from any of his accounts.
>
> **Market Offer**. An open agreement to exchange a given quantity of one unit type for a given quantity of another unit type.
>
> **Recurring Payments**. An agreement between two parties that includes an optional initial payment, followed by a set number of additional payments over a specified period of time.
>
> **Smart Contract**. A customizable agreement between multiple parties, containing user defined scripted clauses, hooks, and variables."

Please see attached white-paper on the BIP47/OT ecosystem which explains Notaries in depth. Presently all functionality is available except for the Voting Pool.

Milestones

The following are milestones for the progress of the project by which the network steward can evaluate the success of the project. The goal of these milestones is to work towards building features that unlock future work throughout the project.

Milestone 1 (Kickoff) - 1 Month

> Instructions: We begin development of a test app with a completed wallet UI supporting BIP-47, OT Notaries (for off-chain transactions) and PKT, BCH, BTC for on chain transactions. In addition, we will simultaneously work on adding PKT support into the OT wallet.
>
> **The coin cost for this milestone will require 5M PKT**

Milestone 1 - 1 Month

At this point, a user will be able to …

Navigate the wallet UI including:

- Initialize / seed their wallet or restore from previous secret words.

- See their on-chain PKT balance.

- See their off-chain PKT balance on a OT Notary.

- Create a on-chain PKT transaction by inputting another user's receive address.

- Create a off-chain instant PKT transaction ("swap") with another BIP-47 user via OT Notary.

- Securely chat with other BIP-47 PKT users.

- Perform above transactions on BCH and BTC.

- Perform all the already implemented OT transactions that are available on a Notary on PKT, BCH and BTC.

The coin cost for this milestone will require 5M PKT

Milestone 2 - 1 Month

Working command line wallet

At this point a user will be able too:

- Perform the above functionality from command line (except for the BIP-47 chat)

The coin cost for this milestone will require 15M PKT

Milestone 3 - 1 Month

Working GUI wallet (minus colored coins/SLP), M PKT

At this point a user will be able too:

- Perform the above functionality with the GUI.

The coin cost for this milestone will require 19M PKT

****

These line items will be proposed for completion on the next NS project window in 90 days and a fresh budget and are NOT included in this proposal's budget of 39m PKT.

Milestone 4 - 1 - 2 Months

Working GUI wallet with SLP/colored coins

At this point a user will be able too:

- Perform the above functionality with the GUI

- Additionally perform SLP token ("colored coin") transactions via both command line and GUI.

The coin cost for this milestone will require 54M PKT