# MONERO REVUO

3Q 2017, Issue 1

## Welcome to Monero Revuo

*Hello everyone, and welcome to the first issue of the Monero Revuo. This will be a quarterly newsletter that aims to give the community an update on the major developments from the primary work groups in the Monero Project. At present, those work groups are Development, Kovri, Community, and the Monero Research Lab.*

*Note: I know that it is September, which actually leaves four months to go this year, and not three, which makes this not a quarterly. By the time I realized that, I had put too much work into this so I decided to bite the bullet and run it, with plans to release the next one four months from now.*

*This is our first time trying this out, so there's plenty of room for learning and growth. Feel free to give your thoughts about how we did and how to make things better. We're really excited to bring this new Monero content to the community. Thanks so much for reading.*

rehrar

## In this issue...


| | |
|---|---|
| Development Update | 02 |
| Monero Research Lab Update | 03 |
| Kovri Update | 04 |
| Community Update | 06 |


## Core Team Corner

This is an opportunity to observe how the Monero Project has grown from its humble beginnings in 2014 to become a major, free libre open source software and de-centralized, crypto currency. In addition Monero has become more than a crypto currency. It encompass original academic research in the Monero Research Lab, a privacy and anonymity I2P router with Kovri and a dynamic and fast growing community. What I find particularly gratifying is that this has been accomplished entirely by donations of funds, resources, time and talent. It is at this point when, I must express my sincerest gratitude and thanks to the developers, researchers, contributors, community members, donors and last but not least to my fellow core team members. It is a pleasure and honour to work with you all.


Francisco "ArcticMine" Cabañas

Credit: @helloluis

# DEVELOPMENT UPDATE

*Underneath the hood, Monero is a powerhouse of technology and code. Work on the code base comes in a variety of ways, from maintaining the current code and fixing bugs to implementing new innovations. Although it's easy to get lost in all the developments of the past few months, and even easier to lose track of all the individuals who contribute and volunteer, we'll take a look at a few development highlights, and what to expect for the upcoming hard fork.*

## Multisig

The community has been anxiously awaiting multi-signature addresses for some time, which would allow for addresses to be made where Monero can only be spent in the event that N/N or N-1/N people sign for the money to be spent. N/N multisig is functional, but is not quite ready to be implemented yet. As well, N-1/N is being worked on, and a successful transaction has been executed. We expect a release sometime in the near future, as both versions will be rolled out together, and will not require a hard fork. Be looking forward to more news in the next quarter.

## Sync Speed Increase

Sync times have been somewhat long for many users, which can be a barrier for users to run their own node. In the upcoming release, syncing has been optimized, leading to faster blockchain sync times, which should hopefully lead to an increased node count. But perhaps the biggest win for the common user comes in the form of bandwidth savings.

## 0MQ

The long-awaited 0MQ, which will revamp the way that the Monero daemon interacts with applications, and provide another avenue for merchants and exchanges to implement Monero, is in the final stages of reviewing and merging. It should hopefully be integrated soon, which would open up a number of options for third-party application developers.

## Subaddresses

What started as disposable addresses - which would allow a user to post one-time use addresses on the internet that lead back to the same wallet - has evolved into something even larger and more user-friendly. Thanks to **kenshi84**, the official Monero wallets should soon support subaddresses, which will allow a user to have multiple different 'Accounts' in their wallet, similar to a bank. This allows for easy division of funds, and allows another layer of accessibility for an ever-growing userbase, while also providing similar benefits of a disposable address if needed.

## OpenMonero

**Jaquee** has spent considerable time preparing the CLI and GUI for working with an OpenMonero backend, which will allow a user to host a node on one device, and easily scan the chain from another for their balance, which is how MyMonero works. The spend keys remain with the device in use, and not the node, although the node has the view key in order to show the correct balance.

## Miscellaneous work

A few more things are being worked on across the board, but we would like to highlight a few of them. A new Esperanto word list was added, **erikd** did some fuzz testing, and **jtgrassie** added readline support for those who won't use rlwrap. There is also a command being added to the CLI which will get current transaction backlog at various fee levels, and issue a warning when a user is making a transaction if there's a backlog.

# MONERO RESEARCH LAB UPDATE

*It was only a few months ago that the Monero Research Lab (MRL) really started picking up speed when the Monero community hired **Brandon Goodell**, a researcher with a PhD in mathematical sciences, to work full time for the research lab on a renewable quarterly contract. Since then, the MRL has worked with researchers around the globe – in places such as Australia, China, Hong Kong, Germany, and Singapore – as well as collaborated with a graduate student from the University of Michigan at Dearborn. Finally, in regard to personnel, the MRL has very recently welcomed **Sarang Noether**, a previous MRL contributor and newly minted PhD in Computational Sciences, onto the team, on a similar contract to **Brandon**.*

## Reading

When delving into the world of experimental cryptography, it's necessary to be up to date on all the recent literature. **Brandon** has worked his way through two cryptography text books and over one hundred peer-reviewed papers. The reading is more than time spent only learning, as the results of those efforts include the preparation of a literature review for publication focused on zero-knowledge techniques, co-authored by **Brandon** and graduate student **Jeffrey Quesnelle** from the University of Michigan-Dearborn. MRL anticipates this publication will be ready by the end of September.

## Research Bulletins

The literature review is not the only publication just over the horizon. MRL will be releasing two research bulletins on the topics of threshold signatures and subaddress schemes, anticipated to be released in early and late September respectively. These bulletins will be descriptive in nature, and will elaborate on work done by **Shen Noether** and **luigi1111** for threshold signatures and **knaccc** and **kenshi84** for subaddress schemes.

## RuffCT

This past quarter, **Tim Ruffing**, a PhD student from Germany's Saarland University, contacted the MRL team with a new RingCT set-up. He and his co-authors (**Thyagarajan**, **Ronge**, **Schröder**) developed a formal definition of RingCT as a cryptographic primitive and present a sublinear implementation that requires no trusted set-up. What does this mean? For the Monero community, it means being able to create transactions with a huge number of mixins, with very little penalty in transaction size, although some definite trade-offs for computational power and time to make said transactions. But for the MRL team, it means working around the clock to put out a complete Java implementation - which is almost complete - for testing purposes. Expect more news regarding RuffCT in the coming months.

## Alternative RingCT

The MRL team was also contacted by well-known researchers and authors on ring signatures and ID-based cryptography - **Shi-Feng Sun**, **Man Au**, **Joseph Liu**, and **Tsz Hon Yuen** - about a different RingCT set-up. Although **Brandon** finds their work 'interesting' and with 'inspired choices', it unfortunately requires a trusted setup, so the MRL has decided to continue with RuffCT. Regardless, it is telling that known authors and contributors to the field are beginning to take notice of the Monero Research Lab.

## Miscellaneous work

Over the course of the quarter, several conversations have been had with various contributors regarding numerous topics such as: view key security, scaling, block pruning, and more. Please read **Brandon**'s August report for further details.

So what does the future hold for the Monero Research Lab? Well, with **Brandon**'s second contract successfully funded, a second PhD on staff, and a number of intelligent, eager volunteers, it seems clear that the future and present technology of Monero is in good hands.

The Monero Research Lab would like to extend a huge thanks to **knaccc**, **kenshi84**, and **Sarang** for going above and beyond in their volunteer MRL contributions. They would also like to thank (in alphabetical order): **Endogenic**, **Fluffypony**, **luigi**, **moneromooo**, **rehrar**, and **smooth** for their work and discussions.

# KOVRI UPDATE

*The battle for privacy rages on many fronts, and the Kovri team is deep in the trenches making sure that the privacy of tomorrow is protected, in Monero and across the world.*

*For those who don't know what Kovri is and how it helps Monero, Kovri is an anonymizing router which will be integrated with Monero. Once integrated, users will have the option to route Monero transactions through Kovri, thus hiding their geographical location and IP address in the process. This will significantly increase the privacy of every single Monero transaction.*

Kovri has seen some exciting recent developments, events, and changes that have lead us even closer to the alpha release. As we summarize the events below, the reader may be surprised to find that many Kovri initiatives are mutually beneficial to Monero as well.

## Promotion, Open Hours, & News Article

**Anonimal** has recently started a deanonymization process so he can further Kovri promotional work. He attended Defcon25 and, soon after, the L.A. Monero meetup; in both locations promoting and describing the importance of Kovri to those around.

As well, Monero and Kovri were featured in an episode of Open Hours hosted by 96Boards where **anonimal** shared about Kovri and how it helps Monero, which can be viewed at https://www.youtube.com/watch?v=b0k5lTMFXBA.

Following the Open Hours episode, a news article was released by BTC Manager which covered the episode and Monero as a whole, but had a fairly narrow focus on Kovri and its use in the Monero ecosystem and beyond. The article can be viewed here: https://btcmanager.com/what-is-kovri-why-is-it-important-for-monero/.

## New Website and subreddit

Along with the official Monero website, the Kovri website was redesigned and launched. The website includes a jekyll localization plugin that works to make sure Kovri instructions and FAQs are in multiple different languages, and serve as a testing ground for implementing localization into the much larger Monero website. You can view the new Kovri website at getkovri.org and contribute at https://github.com/monero-project/kovri-site. Following up with the site redesign, the Kovri subreddit has been revamped to be both thematically consistent with the official website, as well as simple and approachable for any newcomers.

## Documentation Repository

Utilizing the localization plugin for the website, Kovri has launched a repository for Kovri documentation with several folders for other languages ready to be translated. These documents are linked to the Kovri site repository, so editing the documentation edits the individual pages on the website.
This is the first foray into website localization across the Monero Project. The repository is at https://github.com/monero-project/kovri-docs

## Vulnerability Response & HackerOne

**Anonimal** has put together a formalized process for reporting vulnerabilities in both Monero and Kovri, establishing such information as points of contact, processes to be followed, and analysis.
In addition to the documentation, the community has crowdfunded a HackerOne bounty for researchers and hackers to responsibly disclose the discovered vulnerabilities to the appropriate contacts: https://hackerone.com/monero.

## Kovri Video

**Savandra** has been making videos for the Monero community about the technology behind Monero, and up next is the video explaining the Kovri technology and why it's needed. **Anonimal** has been working with **Savandra** to revise the script for the video, and we hope to see it up soon.

*(continued on the next page)*

# KOVRI UPDATE

*(continued)*

### MorrocanMalinois

This summer, the Kovri team bid farewell to FFS contributor **guzzi**, who left to pursue other interests. Although his FFS proposal was left unfinished, the transition was seamless as another Kovri contributor, **MorrocanMalinois**, after encouragement from #kovri-dev, stepped up to finish the remainder of the proposal. The Kovri team is very excited to have **MorrocanMalinois** on board, as his history of contribution has been prompt and helpful, and his work continues to be invaluable to the project.

### Windows Inno Setup (GUI) Installers

**Rbrunner** has enhanced the kovri windows experience by creating Windows GUI installers for easy Kovri installation.

### Contributors

The Kovri team would like to extend a huge thanks to all contributors who have given their time and energy into Kovri. A few shoutouts of note are to the translation contributors (in no particular order): **Dridou**, **Vanchesss**, **MoroccanMalinois**, **erciccione**, **Josexv1**, **serhack**, and **jonathancross**, and a very hearty thanks to **Sarang Noether**, who has given help to Kovri from the MRL. A special award for going above and beyond is given to **anonimal** who wears many hats (lead developer, project lead promoter, mentor, and more) and without whom Kovri would be nothing more than a pipe dream. He has been full-steam-ahead with development, and his ongoing work can be viewed on his github, FFS proposal, and #kovri-dev.

## HELP WANTED

While Kovri continues to make good progress toward release, there is much work to be done. And even after the alpha release, there's much to do to prepare and release beta. The Kovri team would be thrilled to have more hands of any skill level get involved. With this in mind, Kovri is giving an official call to any interested individuals or groups to join us in the development of keeping Monero, and indeed the internet, a safe and private place. Join our IRC channels in #kovri and #kovri-dev with questions about how to get involved.

# COMMUNITY UPDATE

*The Monero community is global, diverse, and full of initiative. It would be impossible to recount everything done by every member of the community for the betterment of the Monero Project, so we will just highlight a few things here. The Monero Project would like to extend a huge 'Thank You!' to every contributing member of the Monero community.*

## Community Workgroup and Meetings

**Justin 'sgp' Ehrenhofer** and **rehrar** jointly started a Monero community workgroup wherein interested individuals can come and work together to make the community an informative and welcoming place to be. They have started running meetings every other week so as to not take up time of dev meetings for unrelated issues. Feel free to check the Issues in the Meta repository of the Monero Project GitHub for the time of the next community meeting and join the conversation.

## Website Redesign

The official website of Monero (getmonero.org) has been redesigned with several new pages added, and the structure updated so as to be navigated more easily. The website has attracted a number of contributors to make User Guides which are being added over time. There are plans to integrate a localization technology in the not-too-distant future. As well, the design of the Monero subreddit has been updated to match the new website.

## Increased Activity

This is an exciting time for Monero as the number of subscribers on the Monero subreddit has been steadily increasing, and the amount of Google searches has been on the rise as well. Also, the number of FFS proposals has been increasing as contributors are looking to spend good chunks of their time developing Monero.

## Europe Promotional Tour

**Justin Ehrenhofer** spent a good amount of his 'study abroad' time in Europe visiting several different countries and giving presentations about Monero. He gave twenty-one presentations in over a dozen different countries to cryptocurrency enthusiasts, and told them about the benefits of Monero.

## Monero Integrations

**Serhack**, a recent addition to the Monero community, opened an FFS proposal to develop Monero plugins for popular Content Management Systems so merchants can easily begin accepting Monero. At present the PHP library has been made and the plugin for Woocommerce has been developed, with Prestashop and WHMCS in active development.
See monerointegrations.com for details.

## Savandra's Videos

At the end of 2016, **Savandra** opened an FFS to create several videos detailing the privacy technologies of Monero in such a way that is accessible to newcomers. After being successfully funded, he has already released several of them, including videos on Monero's basics, stealth addresses, ring signatures, and mostly recently, RingCT. The last two videos (Kovri, and Monero crypto for beginners) are in development, with the Kovri script already well underway.