REVUO MONERO

4Q 2017, Issue 2

Core Team Corner

When reviewing the activities of the Monero Project during 2017 what is most significant is that the degree of progress that has occurred. I will cover some of the highlights; however this is by no means intended to be comprehensive.

In 2017 we saw the addition of Ring Confidential Transactions to the Moreno main chain, first as optional and as of September as mandatory for transactions. Also at the September hardfork the minimum ring size was increased to 5. We now take for granted that hiding the transaction amount is part of the Monero experience, but less than a year ago this was not the case. A very unique challenge was the discovery of a critical bug that affected all CryptoNote based currencies, by a member of the Monero Research Lab in February. This required not only the patching of the Monero code, but in addition the responsible disclosure to other CryptoNote coins. This was completed in an exemplary fashion with no damage to the Monero blockchain. Some other significant events included the redesign of https://getmonero.org/, and the GUI coming out of beta. What will the future bring? 2017 has seen the research and development of some very important future upgrades, including bullet proofs, multi-signature transactions and the ongoing development of the Kovri project.

On the community side there has been very significant growth. This has ranged from phenomenal growth of the Monero online communities, to the regular holding of community meetings and The Monero Coffee Chat. One particularly significant aspect of the community growth has been the growing number of new Monero meet-ups that have been started all over the world.

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. Without you all the remarkable progress we have seen in 2017 simply would not have occurred. It has been a pleasure and honour to work with you all in 2017.

Francisco “ArticMine” Cabañas

In this issue...

DEVELOPMENT UPDATE

Underneath the hood, Monero is a powerhouse of technology and code. Work on the codebase comes in a variety of ways, from bug fixes to implementing innovations. The people that work on the underlying code are just part of the equation, however. Work on the graphical user interface (GUI) also moves along at a steady pace, so users can work with a simple, intuitive design. As a project, Monero has dozens of people working on all aspects of the codebase. We take the time here to look at a few developmental highlights of the last quarter.

Multisig

One of the crowning achievements of the past quarter is the successful implementation of multisig into the Monero CLI wallet, which allows the Monero in a wallet to only be spent if a predetermined number of signers sign the transaction. In the past three months, both the N/N and N-1/N multisig implementations have been completed and merged into the codebase.

Because this is a wallet change, waiting until the next hard fork is not required to use it. One can simply build the current master code from source to start utilizing this feature today.

Bulletproofs

A common theme between development and the Monero Research Lab in this edition of the Revuo is bulletproofs. After the MRL team gave the proverbial nod to switching out the current range proofs with bulletproofs, the development team wasted no time in bringing the new technology into the Monero codebase.

At time of writing, single output bulletproofs are live on the Monero testnet, and multi output bulletproofs under active development. There is still ongoing discussion about whether or not to activate single output bulletproofs for the upcoming hard fork (which, despite multi output being slightly more efficient, would still yield a large reduction of transaction size compared to the current range proofs) or to give this new technology more time on the testnet.

Subaddresses

Subaddresses, another long-awaited feature, have been in the works for a few months now. They will allow the generation of multiple different addresses for the same wallet. In other words, an individual will be able to give out several different address accounts for different purposes, and be able to access all of the received funds using only one mnemonic seed. This increases privacy since, even though stealth addresses hide the actual receiving address on the blockchain, the human element of posting the same public address to multiple sites may tie that address to a user, leading to consequences for some individuals.

Work on subaddresses has completed and, like multisig, is a wallet level feature, so does not need a hard fork, and can be utilized right now if you build from source.

Refreshed GUI

Toward the end of 2017, the community funded **dsc** to implement a dark theme created by **knufflebund** for the current GUI layout. Instead of just being content to just add a new the theme and switch between the two, the GUI team decided to use the opportunity to optimize the current layout to be more user-friendly and accessible.

In addition, work to add subaddresses to the GUI wallet is under way as well, though a release date for this feature is not yet available.

Vulenerability Response

Although technically a workgroup in its own right, the Vulnerability Response group is included here because they don't generate enough content for their own section (the response team is new), but their work is invaluable to the continued security and development of Monero. The Monero Project is committed to providing secure and vetted privacy software, which includes receiving and mititgating reports of potential vulnerabilities in both Monero and Kovri from bounty hunters. You can learn more at hackerone.com/monero to see the great work done by **anonimal**, **luigi1111**, **fluffypony**, and **moneromooo**.

MONERO RESEARCH LAB UPDATE

Keeping up with advances in the space, original research, testing implementations of improvements, providing privacy recommendations, and being the front line of defense against attacks are all part of the seemingly simple job that the Monero Research Lab is tasked with: making sure Monero remains at the forefront of privacy and blockchain technologies. In this section, we take a look at what the end of 2017 held for our two full-time, community-funded academic researchers.

Bulletproofs

One of the biggest excitements of the past quarter has been the work the MRL has done in implementing more efficient range proofs (bulletproofs) into the Monero codebase. Seeing as how the range proofs are the biggest part of every Monero transaction, when bulletproofs are implemented, it will reduce transactions sizes by greater than 80%, which will in turn lower fees which are calculated on a XMR/byte basis. Bulletproofs are expected to go live on the Monero blockchain in 2018.

RuffCT

Correction: Before we begin, the Revuo would like to correct the record on a misstatement in the past issue. We stated that **Shi-Feng Sun**, **Man Au**, **Joseph Liu**, and **Tsz Hon Yuen** contacted Monero Research Lab about RingCT 2.0. This was an incorrect statement based on a misunderstanding within the community about how the paper describing RingCT 2.0 was first introduced to MRL.

Although bulletproofs have taken precedence, MRL has continued their foray into exploring the viability of implementing the RuffCT scheme into Monero. In fact, seeing as how RuffCT can drastically increase number of ring members with the only trade-off being verification times, they have looked into combining the small and fast bulletproofs with the slower RuffCT to allow considerably larger ring sizes with little to no net trade-off. This will even further decrease the likelihood of following outputs through the blockchain and increase the privacy of every transaction made with Monero.

SPECTRE protocol

MRL began reviewing a whitepaper published at the end of 2016 outlining a DAG-based protocol called SPECTRE. At time of writing, there are other cryptocurrencies that utilize a DAG structure instead of a blockchain, but they do it on a transaction level, whereas SPECTRE continues to sort transactions into blocks, and arranges the blocks into the DAG. MRL continues to look at any new surfaces of attack that this might bring, but, while excited about the prospect of a potential protocol change to a non-blockchain structure in the future, the researchers ultimately say more research is needed before they can comfortably surmise whether Monero would benefit.

Multisig & Monero Standards

Brandon spent considerable time turning the informal multisig proposal by various members of the Monero community into a formal cryptographic scheme ready for publication. Further work to complete multisig included review preliminary testing in Java, as well as the final C++ code review.

This aforementioned comprehensive write-up was written for inclusion in what is now known as the 'Monero Standards' document, wherein each standard (i.e. hash function, PoW algorithm, RingCT scheme, range proof scheme, etc.) is elaborated on, the reason it was chosen, and alternatives, as well as their pros and cons. This way, as members come and go from MRL and development, there will be a living, dynamic document from which to easily springboard into further research.

NIPoPoW

The brothers Noether have looked into the possibility of utilizing Non-interactive Proofs of Proof of Work (NIPoPoW) as a way of securely bootstrapping new light nodes. This would allow remote nodes to connect to full nodes and receive only a select few blocks, and being able to trustlessly be assured that all the trailing blocks are correct. This would be useful for brand new remote nodes, but not useful for retrieving previous transactions. Because of the perceived limited use case, there are currently no plans for implementation, but should the need for such a thing arise in the future, it's necessary to have alternative schemes in mind.

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, 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 Project Assistant

The last quarter of the year saw website contributor **rehrar** join the Kovri project as the project assistant manager. Funded by the community via the Forum Funding System, **rehrar** is responsible for website upkeep (a refresh of the Kovri website is underway and should launch within the first month of the year), developer outreach, education, and collaboration with the translation workgroup. **Rehrar** moved from working quarter time to half time in 2018.

Developer outreach began with several universities being contacted toward the end of the year. Unfortunately, it was too late in the semester for students to seriously consider taking on new projects, but bridges have been built and the outreach will resume in 2018.

Development

Kovri continues to move forward on the development front as we march ever closer to the Alpha release. We summarize a few of the developments in Kovri below:

This Q4, kovri saw not one but two i2pd 0days, which are software bugs which are a severe threat that can be exploited, like OpenSSL's Heartbleed. Since **anonimal** had "lost track after 7" count of 0days in i2pd code, he has re-affirmed his stance that all i2pd code must be removed from the kovri code base. This will take more time, but ensures a quality codebase and a minimal attack surface.

A stable testnet is available wherein Kovri contributors can host their own mini-Kovri network locally, so as to test for leaks and bugs without needing to connect to the I2P network at large, or even need internet access at all. It provides a testbed where changes can be vigorously vetted before making it into the main branch, as well as opens up options for security testing without interfering with a parallel running main I2P net. Other benefits include allowing for work to continue offline for contributors who wish to remain off the internet during testing

Another area of development has been the construction of a prelimiary API. This is essential for third-party applications, such as Monero, that want to connect to the I2P network using the Kovri router in the future. With these first steps taken into the creation of the API, the promised future of Monero's continued privacy seems brighter than ever.

The above mentioned work are merely highlights of the past quarter. For information on further work completed, please see the Kovri repository on Github.

Research / Review / Collaboration

As a budding anonymity technology, Kovri has decided since its inception to be at the forefront of all technological anonymity advancements. Time is set aside specifically for review of papers, new technologies, and other research related to mixnet tech. As well, in order for Kovri to be secure, all pull requests must be vigorously reviewed, especially those of newcomers, keeping the level of trust at a mimimum. Lastly, Kovri has collaborated with the Monero Project at large on several fronts, including the Monero Translation workgroup, the Monero Research Lab, and the development team, not to mention close collaboration with software dependencies like Crypto++ to ensure secure software.

Contributors

The Kovri project would like to thank all contributors who have given of their time, energy, resources, and money to Kovri in this past quarter. In particular, they would like to highlight **anonimal** for always going above and beyond, **rehrar** for his continued and enthusiastic support, and **MoroccanMalinois** for his contributions. Kovri would also like to extend a hearty welcome to the newest recruits, **selsta** and **oneiric**. We look forward to their contributions, and are pleased to have them in the Kovri family.

COMMUNITY UPDATE

The Monero Community workgroup started in 2017 and has continued in full force. Their primary goal is to identify needs from within the Monero community and fill them, this can take a variety of forms, such as educational materials, community engagement initiatives, user guides, and more. Community is an open workgroup, and anyone that wants to see the community improve can join by visiting the reddit /r/monerocommunity, or by attending one of the biweekly meetings (details on Github).

Meetings & Coffee Chat

A small, but commendable achievement of the community workgroup is the continued bimonthly meetings that takes place in the #monero-community IRC channel. These are open meetings where anyone can contribute to discussions that pertain to the community aspects of Monero.

A second gathering in the same vein was started by **Justin 'sgp' Ehrenhofer** called the Monero Coffee Chat, in which community contributors join a livestream conversation each month to discuss development, community projects, Monero philosophies, and other relevant information. These new chats intend to make Monero contributors more accessible and allow people to participate in a more personal way than just text alone.

Taiga & Mattermost

Because Monero is a grassroots initiative without a central leadership structure, all development, coding and otherwise, is dependent on workgroups completing various tasks within their expertise and passion. The Core Team saw fit to invest into, and provide the resources necessary for these workgroups to organically form and carry out their vision for Monero. These resources are Mattermost (an open-source, self-hosted Slack alternative), and Taiga (an open-source, self-hosted agile development platform), with more resources under review for the future. See the 'Hangouts' page of the getmonero.org website for details on accessing these resources.

Monero Integrations

Serhack and **cryptochangements** continue working on creating open source plugins for various websites so merchants can easily integrate accepting Monero as a payment option for their goods and services. The past quarter saw the release of the WHCMS and Magneto plugins to add to the already released Woocommerce and Prestashop plugins. A plugin for OpenCart is expected to be released in 2018.

Educational Videos

Savandra continued working with community members to create accessible, easy-to-understand videos for newcomers. The Kovri video was recently released after months of contributions, and the script for the Monero involvement video is under way. These videos add to existing ones about Monero's basics, stealth addresses, ring signatures, and RingCT.

Monero Meetup Kit

During an open ideas time at a community meeting, **serhack** suggested creating a "meetup kit" to give to interested groups who would like to learn more about Monero. This resulted in the culmination of a month of work to get the necessary materials. These include paper wallets and activities that show how to use several wallets, webcam covers, stickers, infographics, and tri-fold handouts. The project was funded by generous donors through the Forum Funding System. **Justin** distributed these kits to several organizations throughout the United States.

Monero Translations

The Monero Translations workgroup formed at the tail end of 2017 with the explicit purpose of localizing all Monero materials, from website to GUI to pamphlets. Since its inception, **ErCiccione** has led the team to translate the GUI into 5 more languages and fix existing translations, and translate the Kovri website and Monero daemon. If you're interested in helping, you can visit them at the #monero-translations IRC channel, or see their project on Monero's Taiga instance for translation guides, a wiki, and an issue tracker.

KASTELO UPDATE

*Kastelo is a project started by **msvb-lab** whose primary goal is to create specifications for an open-source hardware wallet in which cryptocurrency users could keep their Monero. While Kastelo is a new workgroup on the scene, the progress of their work is nothing short of amazing, with their past three months of work already showing great promise.*

Funding & Taiga

On August 19th of 2017, **michael** posted a proposal on the Forum Funding System (FFS) about making a dedicated hardware wallet. Until this point, Monero has had no hardware wallet support from the major providers, despite ongoing development from said providers. Still, the idea of having a completely open-source - from hardware to firmware - hardware wallet was appealing to many, and the proposal was quickly funded.

Michael took advantage of Monero's new workgroup resource offerings and set up an area for the wallet in Taiga which, at time of writing, has attracted 33 different contributors ranging from Mechanics to Layout to Testing. All updates to the project can be viewed on Monero's Taiga instance.

Prototypes for the Holidays

After a couple of months of hard work, **msvb-lab** and team made terrific progress, and came out with a few working prototypes. After a small sign-up process, the team sent out roughly 30 prototypes to eager testers.

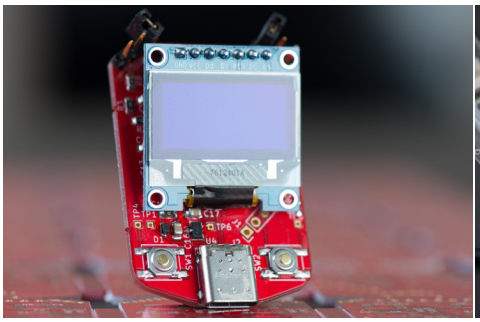
It should be mentioned that, as they were prototypes, all testers were warned not to try to keep their cryptocurrencies on them, which would have been difficult anyway because of the fact that it did not ship with anything other than the most basic of firmwares. Pictures of these prototypes are shown at the bottom of this page.

34C3 Conference

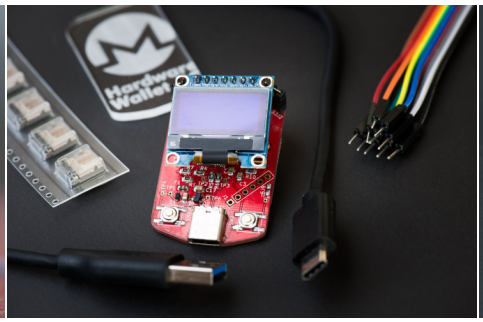
Michael joined the group of the Monero community that attended the 34C4 conference and presented before other conference attendees about the project and its progress. He had a few more prototypes to distribute to interested individuals at the conference.

Workgroup Meetings

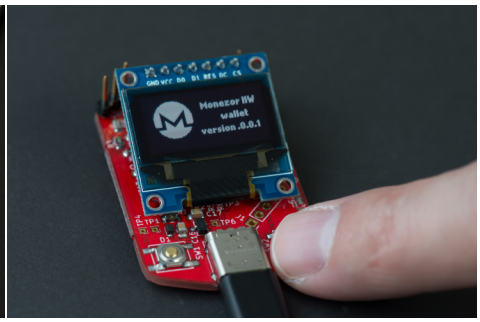
Kastelo requires several mini-workgroups working simultaneously to turn it into a reality. To date these subsets of people include small teams for QA testing, firmware, mechanics, FPGA design, and logo/branding. All of these teams meet in monthly meetings, where everyone starts out in a large group for general discussion before breaking off into their groups to target their areas of expertise and give each area the discussion they deserve. The logs to these meetings will be posted alongside other workgroup meeting logs on the getmonero.org website.



The hardware wallet prototype



Glamor shot



Wallet booting basic firmware

MONERUJO UPDATE

*Monerujo is a fairly recent workgroup led by **m2049r** and his renegade band of Monero pirates. They hold the achievement of being the first group to bring a fully-featured SPV wallet to Android phones, and are looking to expand even further into other areas. Their success sets an example for other workgroups to come.*

Android Light Wallet

Monerujo started when **m2049r**, a relative newcomer to the Monero community, posted on Reddit in August about working on an Android wallet. Over the coming months, he single-handedly succeeded in completing a fully functioning SPV wallet and getting it onto the Google Play Store as beta software.

It wasn't long before a team started to form around Monerujo, including UX/UI designers, graphic designers, copywriters, and project managers that made the next release not only functional, but accessible and aesthetically pleasing.

The wallet can be downloaded from the Google Play Store, and users can visit **monerujo.io** for more information.

XMR.to integration

In November of 2017, the administrator of XMR.to (a community-trusted service that pays Bitcoin addresses after you send an equivalent amount of Monero to them) contacted **m2049r** about integrating XMR.to into their wallet. Seeing no downside, the Monerujo team launched the integration.

At present time, Monerujo users can either paste a XMR or BTC address into their send fields or scan the QR codes of either cryptocurrency, with the BTC conversation taking place in-app via XMR.to API. This means the Monerujo wallet can be used anywhere Monero or Bitcoin is accepted.

Hardware Wallet Firmware

As noted earlier in the issue, the Monero community successfully funded the development of an open-source hardware wallet where they can keep their Moneroj safe. While the progress made by the Hardware workgroup is both swift and exciting, it should be noted that the Forum Funding System proposal just covered the development of the specifications of the hardware, not the firmware.

The Monerujo team has jumped at the opportunity to further involve themselves in the success of Monero, and, near the end of 2017, made the decision to start development of a firmware option that users can deploy on their Kastelo wallets.

HELP WANTED

Monerujo is currently looking for knowledgeable and passionate individuals who would be willing to help develop Monerujo for both F-Droid and iOS. If anyone would like to help, please come join the Monerujo public chat in Monero's Mattermost instance at mattermost.getmonero.org and ask for **m2049r**.