About Privacy on Monero and Lightning: Interview With Riccardo Spagni

Tobias W. Kaiser ⋮ 10-13 minutes ⋮ 10/27/2020

BeInCrypto recently caught up with Riccardo Spagni, also known as @FluffyPony, to talk about the state of privacy on Monero and the Lightning Network.

BeInCrypto: Welcome, Riccardo, and thanks for your time. First of all, can you tell us something about your specific role at Monero? **Riccardo Spagni**: As part of the core team, I started off as the lead maintainer, right at the beginning of Monero. I worked as the lead maintainer for about six years and then stepped down from the lead position towards the end of the last year to focus on Tari. I'm still working as one of the maintainers, though.

Monero Has Multiple Models to Compensate Developers

BeInCrypto: It is often unclear how open-source projects compensate their developers, especially when people spend the majority of their time on the project. How does Monero solve this? **Riccardo Spagni**: There are several models for how developers are compensated. Even within Monero, we use different approaches. As in most open-source projects, the majority of our developers consist of volunteers, who help out in their spare time, or when they have free time as part of their job. Secondly, a company can sponsor someone to work on Monero. For example, there are companies like XMR.to, mineXMR, and others who have paid developers in the past to work on Monero, and some of them still do. The third way is quite interesting and somewhat unique to Monero. Monero has a crowdfunding system where teams or individuals can propose that they want to build a particular feature or just work on Monero for a few months. They can then raise funds in XMR from the community. Formerly, this has been called the

Forum Funding System (FFS), when it still ran on the Monero forum. Now that it has its own section on the Monero website, it is called the Community Crowdfunding System (CCS), and there are tons of activities there, lots of interesting proposals, and lots of proposals that have been fully funded. This has been going quite successfully for about five years now.

How Can We Reconcile Regulation With Privacy?

BeInCrypto: Right now, privacy coins are fighting on three different fronts: there is regulation, then there's tracing companies, and thirdly, there is adoption. Let's talk about regulation first. While governments and regulators can't shut down Monero directly, they can at least hinder its progress by pressuring exchanges to delist XMR. How are you trying to reconcile regulators' demands with privacy? **Riccardo Spagni**: There are a couple of aspects here. Tari Labs has worked together with Perkins Coie, which is an international law firm, to put together a regulatory whitepaper, which helps regulators, law enforcement, exchanges, and others who deal with privacy-focused cryptocurrencies to have some understanding about how they can comply with existing legislation and still interact with these cryptocurrencies. This also includes payments over the Lightning Network or deposits made with CoinJoin obfuscation, so it does not just apply to Monero. The paper came out about a month ago, and so far, it has been quite successful, especially getting a lot of interest from exchanges. Ultimately, regulators need to be educated, and they need to understand that, to a large degree, privacy coins are like cash. Cash is not an anti-law-enforcement thing or an anti-government thing, and it's perfectly compatible with existing regulations. Regulators need to learn that having a publicly traceable currency is not good for anyone. It's not good for governments, it's not good for individuals, and it's not good for businesses either. Actually, privacy is what governments, individuals, and businesses want.

Privacy Is a Permanent Cat and Mouse Game

BeInCrypto: Besides regulators, there are tracing companies that might potentially jeopardize privacy by tracking transactions. Less private coins

like Dash or Zcash have already fallen to Chainalysis. Recently, CipherTrace claimed to be the first company to track Monero transactions. Even the IRS is offering bounties to crack privacy coins. How far do you think Monero is ahead in the race against tracing companies? **Riccardo Spagni**: CipherTrace is a particularly great example, but when you are talking to them, you find out that they are not as successful as they claim. There was an interview with their CEO, where they showed a screenshot of what was basically a visual block explorer for Monero. By their own admission, this is based on heuristics. They claim to have 90% confidence in what the true output for a transaction is, but this is a totally arbitrary guess. This is not to say that Monero does not have any weaknesses. But all these are discussed openly. There is plenty of information about how you can combine good OPSEC with Monero to improve your privacy, but it's fair to say that Monero is not perfectly private, and it's never going to be perfect. But at this point in time, I can confidently say that there is no critical breach that reveals all transactions. Some transactions may be weaker than others, but generally speaking, Monero provides pretty good privacy. With the IRS, they are not just interested in Monero privacy but also breaking privacy on Lightning transactions. So it is clear that regulators have some idea about how things should work, like that all things should work like Bitcoin without any privacy tools such as CoinJoin. They want everything to work like a bank, where they get a feed of data from all transactions, and the staff is obligated to report suspicious transactions. I think ultimately, they are going to end up realizing that they will always be on the backfoot because privacy is not a state you achieve at some point. It's a constant battle where we are constantly aware that attackers are hovering over our shoulders. This attacker does not necessarily have to be the NSA, or the CIA, or some other three-letter acronym. The attacker could be a fifteen-year-old kid in Poland who discovers a bug in your code or an organization like CipherTrace. The attacker could also be a hacker that is motivated by other things. This is not about imagining that the government's regulators are out there to break Monero. It's about accepting that with cryptography or privacy. You always play that cat and mouse game. You always have to stay alert and remember that there is someone out there trying to break your privacy, and you have to stay ahead of that. **BeInCrypto**: With the Lightning Network, it's not possible to trace any transactions on the network from the outside. What does this mean for privacy? **Riccardo Spagni**: There has

been some really good research on that lately. The biggest challenge is using Bitcoin as a settlement layer. When a Lightning channel closes, you can see how the balances change on the Bitcoin blockchain, and you can infer a lot of information from that. So there certainly are weaknesses in Lightning's privacy. This is not surprising, though. The guys at Lightning Labs and other developers are very open about the current state of Lightning privacy, and because they are open about it, they also work on improving it. I'm very hopeful that Lightning will continue to beat the drums of improving privacy. I do think that there is a large portion of users who make very small and very arbitrary transactions, like buying a coffee, which could benefit from the privacy the Lightning Network can provide. There doesn't have to be a substantial focus on privacy because their primary focus is security and scalability. But I think that there definitely could be a point in the future where Lightning privacy is sufficiently high, and I think that's where things are moving.

Cryptography Services Need Better UX

BeInCrypto: This brings me to my last question. Any privacy feature from cryptocurrencies or cryptography, in general, requires a high number of users. When this isn't the case, the people who do use privacy features tend to stick out even more. Over the last year, it became relatively clear that most cryptocurrency users don't really care that much about privacy. Do you see this as a problem, and if so, what can we do about it? **Riccardo Spagni**: I do agree that there is generally a lot of apathy towards privacy. In terms of what we can do about it, something that I try to get people to do is the six-month privacy challenge. This means every six months, you take one service that you use that is not private and try to replace it. For example, can you get rid of Instagram and still send your friends pictures by using some service that is privacy-preserving. If you're on Facebook, can you get off Facebook? If you're locked into Gmail, can you get rid of Gmail and use Tutanota or Protonmail instead? When you take just one thing every six months, it's not as disruptive, but it gives you a scope to make at least one major adjustment and get used to it. I think that encouraging people to do this is a step in the right direction. The other thing is simply a reality that is pushing people towards privacy-enhancing technology, just by virtue of the steady stream of hacks and leaks that we see all the time. This

is not to say that if everyone used Monero or Lightning, that there wouldn't be any data leaks at all. But it's much harder to leak information if you don't have any information to leak. We're kind of in an interesting place. There have been so many hacks already, and people are almost aggravated enough to get off Facebook or Instagram, but they just need that last little push. But I do think that we are seeing more and more people waking up to the fact that it's time for a change and that it's time to take your privacy back. I mean, we close the toilet door when we go to a public restroom, and that is not because we are plotting to overthrow the government. It's just that we don't want people to see us on the loo. I think that people are starting to realize that privacy is just a natural state. It is not a weird thing to want to have some privacy. There is one more thing that I would like to add. As technologists, we have created somewhat of a poor situation where the user interface of most privacy-enhancing technology is just rubbish, and that is on us. We need to acknowledge that we have failed to create user-friendly interfaces. A lot of really good privacy-enhancing technology requires a deep understanding and use of the command line, and that is just not fantastic. One thing that will help in adoption is improving the user experience, and there are already some companies that are working on this. So I'm hopeful that this will get better over time. **BeInCrypto**: Thank you once more for the interview. **Riccardo Spagni**: Thanks so much for your time. Cheers!

Disclaimer