Hi Everyone! Now that I have your attention, this post is not short, but neither is the title misleading. I genuinely believe there is enormous potential here. Please give it a read and let me/us know what you think.

Background

I'm leading a project with others in the community, and we want to gather feedback on a future SCRT community spend proposal. Over that past few months, we've finalized details and are looking forward to building in earnest. We feel that the success of this product will have a huge impact on both the Enigma community and the value of SCRT tokens.

Proposal

Enigma is creating the framework for private blockchain transactions, but the community will not grow until apps are using that framework. What better place to start than private key management? There are many private key storage options available today, but they all share one problem - a single point of failure. Private key distribution is a revolutionary way to store crypto assets across multiple devices, even untrusted devices. It is more secure and more convenient than any other option.

How many stories have you heard about someone losing millions worth of crypto? Securely storing a private key is complicated and tedious, even for the most technically savvy people. There are numerous backup options, but even the most advanced options still have a single point of failure. The wrong mistake might mean the loss of everything. Take the mnemonic phrase backup strategy. This tool is useful if you lose access to a personal wallet and want to recreate it, but it is still a single point of failure, not to mention a large vulnerability. What happens if you lose your backup phrase? What happens if it's stolen? No matter how you store crypto, there are critical points of failure with each option.

Maybe you've decided to go a different route and store your assets on a cryptocurrency exchange instead. Surely they have better security practices. They must be better than they were in the past, right? Probably, but let's not forget one important point. When Mt. Gox was hacked, the first thing they did was stop withdrawals. Even though funds were still available, owners got nothing because Mt. Gox "said so". Hacks still happen all the time. Exchanges make mistakes too. When that day comes, don't act surprised when the exchanges take care of themselves first.

Regardless of where you store your cryptocurrency, all solutions have problems. You can manage the crypto storage yourself, or you can give up control and put your trust in an exchange. Either way, if your choice fails, you've lost everything.

The answer is to split and distribute a private key across multiple hosts. By storing private keys with multiple parties, we can ensure they are never lost, never stolen, and most importantly, always in your control. We can split a private key into shares and distribute a single share to each host. A single share or even multiple shares does nothing until a minimum number of key shares are combined. This framework means keys are never lost, and never stolen unless the entire network is compromised (even then there are safeguards). You can have the benefit of truly secure key management while retaining control of your assets at all times. You'll never have to trust a third-party again.

A solution like this benefits everyone since it works for every cryptocurrency. It's a universal solution! It is as easy as the best options available today and more secure than any of them. It embodies the culture of the crypto community by returning control back to the owner and eliminating the centralization of wealth that plagues all modern financial institutions, including cryptocurrency exchanges.

Specifically for SCRT token holders, this product will bring astronomical growth to the community. By using Enigma to store the wealth of Bitcoin and other cryptocurrencies, we will increase network usage and valuation by many orders of magnitude. Enigma's protocol is making the next generation of blockchain applications possible; we are making that possibility a reality.

What's next?

Currently, there is more than 550,000 SCRT in the community spend pool. These funds are set aside for "improvements to the community" in whatever way the community deems appropriate. Some of the funds are earmarked for the ENG-to-SCRT conversion, and we can all agree that is the most important task by far. However, there are still funds available, and we feel this project is an excellent use of those funds.

Many of us are working on this, but we have full-time jobs that take the majority of our time. We want to put 100% of our efforts into this, so we are here asking the community to make that possible. If approved by the community, we calculate that this will require 400k SCRT and six months to complete. It is important to note that this request is a grant-like proposal with SCRT paid upfront rather than a bounty-like proposal with SCRT paid upon completion. This option allows us to incentivize the right people and is similar to other grant-like funding where funds are given upfront with the expectation of future returns. The returns, in this case, are the growth of both Enigma and SCRT. All code developed with these funds will be open source and available to the community.

We are looking forward to hearing everyone's thoughts and are excited to be here, at the beginning of the SCRT era, just waiting to take off.

TL:DR

- We have a plan. Vote to invest 400k SCRT in that plan, and we will not only build a product that benefits everyone in crypto but will also move the decimal point of SCRT a few places to the right. Please join the discussion and provide your thoughts!