Philosophy

When the first cryptocurrency Bitcoin was imagined, it had the benefit of being a novel idea which paved the way for a framework of currencies, products and services that now make up the entire cryptocurrency ecosystem. Today new coins and projects are popping up like weeds, mostly due to greed, but partly because people are driven to innovate and conquer new realms and markets. Our mission and vision are to create products and services that have real-world benefit and use-cases that will provide consumers, merchants, and investors with legitimate security, ease of use and practical implementation and management despite technical ability. We understand that the cryptocurrency sector will ultimately be legitimized and integrated into global commerce ubiquitously by simplistic design, implementation and accessibility. With that perspective in place we will continue to add novel products and services offerings to ensure complete market integration and consumer access.

First and foremost, it is important to understand that without secure products and services the entire cryptocurrency framework is at stake and will crumble at the whims of disruptive and malicious actors (i.e. hackers and scammers). This project has been designed from the ground up around these values and has proven this by creating a system of trustless peer-to-peer interaction to mitigate one of the most common attack vectors – fraudulent direct currency trades. The escrow service that we have created and combined into our currency wallet is an example of how conglomeration of products and services can enable users to choose more secure methods of transaction by default due to ease of accessibility. As developers and market facilitators we must remember that consumers, merchants and investors may have little to no understanding of security or exploitation. The responsibility of creating a safe environment should ultimately rest in the hands of those who are contributing to and maintaining the ever-growing cryptocurrency framework.

As the various sub-sectors and markets of cryptocurrency evolve and expand it is necessary to provide as many use-cases as is possible to foster the freedom and personal anonymity that was intended for its patrons. In this spirit we offer

a peer-to-peer escrow service that preserves the privacy and freedom of those who want to trade one type of currency for another. Accessibility to a means of transacting cryptocurrency is improved over the traditional internet exchange by allowing users to simply download the software from anywhere at any time. Because users are not required to register to be able to use the escrow service they may remain relatively anonymous as they make transactions. Additionally, due to the disparate nature of the escrow, patrons have the freedom to trade coins at any exchange rate that they can agree upon, releasing them from the constraints of the traditional exchange systems.

Consumers, merchants and investors must continually be educated about the dangers of malicious actors in both physical and cyber realms, but it is unquestionably the responsibility of the organizations that are providing framework products and services to create improved security through design and better user experience. Many of the issues plaguing patrons in this initial phase of growth for the cryptocurrency market are due to overly technical setup and management of complex software (e.g. wallets and nodes). In turn, these overly complicated systems cause users to reach out for assistance in configuration and management, which has made them vulnerable to exploitation such as phishing or downloading malicious executables. One of the major flaws that is continuing to foster this problematic environment is faulty or incomplete software design and compilation. So-called “developers” that produce software and create currencies by forking public cryptocurrency repositories who lack the knowledge to properly distribute sound code are a blight to the entire community. To resolve this issue consumers should consider the basic software offerings of a project to meet a minimum standard of requirements: statically compiled wallets that do not require additional download of supporting libraries, seed nodes are in place so that users do not have to add nodes in their wallet configuration files and valid security certificates (e.g. SSL) are in place and up-to-date. We intend to form a community-based committee that will validate projects’ software at a base level and provide feedback to consumers to help them make more informed decisions.

In summary, the cryptocurrency market sector and global community is still in its infancy, but it is time to nurture its growth and push it along to the next phase

of evolution. We are committed to bringing new products and services to market that will provide secure, easy-to-use, practical applications for consumers, merchants and investors. It is our mission to legitimize and solidify the foundation and integration of cryptocurrency throughout all global market sectors. We are XCGtech, and we are here to help you trade with confidence.

Technical

Because vulnerability is practically inevitable, when we designed Xchange with two custom SPORKs [1] specifically purposed with stopping exploitation at a moment's notice.

The **Escrow SPORK** is designed to disable the escrow functionality on client wallets if a critical bug is discovered, the back-end framework requires a major overhaul, or any part of the system is compromised by a malicious actor.

The **Kill Wallet SPORK** is designed to disable syncing and cause an error at wallet launch if the client version does not match the SPORK version on the network. This a "worst case scenario" functionality which we've put in place because we have seen far too many blockchains suffer at the hands of exploitation.

These functionalities are enabled and disabled by the WIF format key of the private **SPORK** hard coded in the wallet.

We chose the **LWMA**[2] difficulty retargeting algorithm after months of research and testing with time stamps, block height, and hash rates using CPU and GPU mining rigs. We found that this algorithm coded by Zawys was the best fit for **Xchange**.

Using the GPU's and CPU's we tested the Xchange network by providing certain rigs 51% or more of the hash rate and we found no 51% hash rate attack problems. As we kept mining we also found that the difficulty was properly

[1] A SPORK is a mechanism invented by the DASH crypto-currency that is used to safely deploy new features to the network trough network-level variables
[2] Linearly Weighted Moving Average

adjusting to the hash rate. From all the data gathered we decided that the **LWMA** is the best difficulty retargeting algorithm currently available.

When considering what algorithm to use for **Xchange** we took into account that a large part of the cryptocurrency community is made up of mining enthusiasts and we wanted to give them a quality product worthy of their scrutiny. After much deliberation we decided to proceed with the **X16R**[3] algorithm designed by the developers of **Ravencoin**. The benefit of **X16R** is that it is *ASIC resistant*, which falls in line with our focus on keeping the power in the hands of the people and maintaining a decentralized system.

The Masternode system that we use is entirely different from what other MN coins use. We decided to make the MN as more of an investment system rather than a capital system. We were able to accomplish this by reducing the block rewards and increasing the MN collateral. **50,000 XCG** is needed to run a masternode, with this regard it makes it very difficult for someone to easily obtain one. We did this so that serious investors would consider purchasing one to be a logically sound and fiscally worthy venture. Investments should be studied and thought out not just for a return on investment but more about the potential of the coin and its applications.

The large collateral combined with reward stabilization allows us to maintain a lower rate of inflation by limiting the production to approximately *110 nodes per year*. Another reason we picked **50,000 XCG** was to discourage exploiters and hackers from attempting to damage the system. Coming up with **50,000 XCG** would be something hard and a costly venture just to experiment with exploitation.

The use-cases for our MN that we implemented are: a donation node for charities, and a “stable” MN with no fees to lock up XCG and help stabilize it for the first year. The stable node is a collection of the community’s coins, so in essence, they are able to user their currency to help strengthen the long-term consistency of the market while still being able to reap the rewards of their investment.

[3] https://ravencoin.org/wp-content/uploads/2018/01/X16R-Whitepaper-3.pdf

Escrow

How the **Escrow** system works:

Step 1. Download the Xchange wallet
Step 2. Purchase Xchange coin (**XCG**) through the wallet directly, by escrow, or through an exchange
Step 3. Find someone to trade coins with
Step 4. Create an escrow request
Step 5. Connect your request with the other party's request
Step 6. Submit payment to the provided escrow wallet address

For more information about the Escrow functionality, please refer to our guide.