AMITY COIN PRE-WHITE PAPER

v 1.1: 04.13.2019

@hooftly, @papacabeza

Abstract: *AmityCoin is a community-based research project for decentralization and privacy. We're not ready yet for a full-fledged white paper so we are outlining our architectural plans and anchoring principles in our preliminary white papers so as to give the community some material on the sponsors' philosophy and plan and to create a record for the project. In this updated version we update about exchanges; discuss our chain substitution by a fork to a new chain based on Nerva; our interim learnings on quantum resistance adaptation; and we produce the project's first treasury report.*

Table of contents

0. Introduction

As we described in our pre-white paper v 1.1, AmityCoin is an early stage project that is focusing on principles of decentralization, anonymization, privacy and quantum resistance. We expect the technical work on our project to continue (together with our miner community) for another eighteen (18) months before we feel that the project will be ready for user adoption (miners aren't "users" in the ultimate sense). Our project will be awesome when we're done but we want to hack on it together with our community to make AmityCoin unique. In this update to our pre-white paper, we make several announcements.

1. Miner liquidity

The community has added two centralized exchanges (cratex.io and offshorex.exchange) and one decentralized exchange (bisq.network). Our position on exchanges remains: always be cautious. Not your keys, not your coins. Here's our guide.

2. Fork to Nerva's codebase

We're forking (i.e., requiring a chain substitution) to Nerva's codebase to better achieve our goals in privacy and decentralization as well as keeping the original mission statement of GPU and Pool Resistance. A chain substitution is a major operation. Because we're going to do this substitution and possibly at least one other (i.e., when we move to a quantum resistant model), we are proposing a repeatable, audited chain substitution plan.

Why chain substitute at all

AmityCoin is focused on certain principles and on using whatever the best technology is to deliver them. Our top three principles are privacy, anonymity and decentralization. Because we're developing a project that will last for generations the most important paradigm for that is the project may carry different technical shells over time. If our project lasts for the 2,000 years that the PoW cycle calls for, there will be multiple chain substitutions in the centuries to come. The important thing to keep in mind is transparency and keeping the process auditable while maintaining the projects core principles.

Chain substitution + ZPM simulation

AmityCoin is a zero-premine (ZPM) project and the chain substitution will not change that. However, because newAMIT will be on a different chain, the users will need to buy into the new chain with oldAMIT. In order for this to occur, we require an allocation of newAMIT that is equivalent to the amount of oldAMIT currently in circulation. Our audit will demonstrate that the newAMIT chain has the same zero-premine characteristics as oldAMIT.

Monero + Masari

The Nerva codebase is an adaptation of Monero and Masari. Users can expect the privacy protections of Monero and Ring CT as well as the benefits of Bulletproofs V2. This also brings Multi-signature wallets to AmityCoin.

Main substitution

Timing for the main substitution/swap(i.e., via cratex.io) will be from **May 1** to **May 30, 2019**. We plan to work with cratex.io and ask users to sign up to Cratex using whatever email they like. Cratex doesn't require KYC so any email will suffice. Cratex will create two AmityCoin wallets on the exchange and when it comes time to swap users will deposit into their oldAMIT account and once it comes time to substitute users will be credited with newAMIT in their new accounts.

Secondary substitution

If anyone misses the main substitution/swap window, we'll have an opportunity for a more manual swap to occur from June 1 to August 31, 2019. We will describe this process before the launch of it. **There will be no opportunity to substitute after August 31, 2019. Any newAMIT that has not been swapped by August 31, 2019 for oldAMIT coins will be burned.**

The Burn

Since we love a good burn we will hopefully have some newAMIT to burn. On September 2, 2019, we'll burn any remaining newAMIT from the allocation that isn't substituted by then.

Audit

We will ask an identified auditor to review the blockchains of oldAMIT and newAMIT. The auditor will certify the following <u>four</u> controls:

- Assure that oldAMIT supply and newAMIT allocation is 1:1 for the block height on May 1, 2019;
- Verify the total amount of oldAMIT swapped for newAMIT as of May 30, 2019;
- Verify the burn on Sep 2, 2019.
- The old Blockchain will be kept and backed up in multiple locations. This will be available in the form of an explorer so the old chain's transactions and blocks can still be explored and audited.

3. Quantum Resistance

There's been a snag in our analysis of quantum resistance: there's nothing ready yet for implementation on a privacy chain. In order for us to implement quantum resistance today, our tradeoff would require us to give up on privacy and anonymity, and that's not a constraint that we'll bend on. In one analysis, the project QRL looked at implementing Zk-Snarks and concluded that applying QR to it would turn a 2.1 kb transaction into 400 to 500 kilobytes. We're still committed but our preliminary conclusion now is that we may need to let the development occur further with QR and watch the NIST competition before we implement it.

4. Nerva collaboration

We're forking from Nerva and we intend to develop a few projects together for each other's mutual benefit. The first place that you will probably see that occur is in our collaboration on new Mobile and Web Wallets. More on the collaboration to come.

5. Mining

There will a few changes with the way mining AmityCoin is handled.

Mining with multiple machines

A lot of AmityCoins miners use multiple machines by connecting miners to one local node remotely through the RPC which only requires a user to have one daemon running and synced to utilize multiple machines. This will no longer be the case with the new chain as every miner will be required to hold a local copy of the blockchain.

Mining Software

There will no longer be a separate miner independent of the daemon and will instead be handled by a command from within the AmityCoin daemon.

Block Reward and emission

AmityCoins new chain will be a little different in terms of how the coins are emitted. Instead of using an emission factor and an *extremely slow* decreasing block reward we have decided to use what we are calling a static block reward. Each block will give a reward of 186.000000 coins. We will be moving to six decimal places from the current four. This will allow us to control the emission period and tweak it if necessary.

6. Treasury report & sponsor funding

The best thing that the sponsors of a decentralized project can do is provide transparency to its community about their own financial movements. That's because people that may have inside information have a tendency to act based on that and this can give outsiders the shaft. We don't like the shaft. We've decided to give some transparency and voluntary lock-in for our own holdings.

Why lock-in

We're locking these funds up for a simple reason: an anonymous sponsor/miner that has told us that they would contribute funds to us on occasion but only on the condition that we have a lock-in period for funds of one year. This is roughly modeled on the one-year retention period for key personnel given options in securities laws. We're happy to accept it -- however, because of our swap, we're late in implementing it. These are the sponsor grants (remember, these are not part of the allocation, they're previously mined or exchanged):

@Hooftly:	725,000 AMIT [17 March 2020]
@papacabeza:	500,000 AMIT [17 March 2020]
@hhbzou:	500,000 AMIT [17 March 2020]
@JerMe404	20,000 AMIT [17 March 2020] [tech collaboration]
@AngryWasp	20,000 AMIT [17 March 2020] [tech collaboration]

Terms: None, other than lock-in. AmityCoin is not seeking any commitment from the sponsors for these contributions. But hopefully, these kinds of things will keep the sponsors and community vested and engaged.