AMITY COIN PRE-WHITE PAPER
[v 1.0, 02.20.2019]
@ChrisChaos + @papacabeza

Abstract: *AmityCoin is a community-based research project for decentralization and privacy. The project has been taken over volunteer sponsors who are interested in furthering the development of the coin based on long-term principles and goals focused on decentralization, privacy & security and quantum resistance.. It's too early for a full-fledged white paper so we outline those principles and goals in this preliminary white paper so as to give the community some material on the new sponsors' philosophy and plan.*

0. Coin Specifications

The coin's basic specifications are listed below.

Name:	AmityCoin
Ticker:	AMIT
Release:	Nov 5, 2018
Algorithm:	Cryptonight Soft Shell V2 (tweaked)
Proof Type:	PoW
Website:	https://www.getamitycoin.org/
Code:	https://github.com/CalexCore/AmityCoin
Explorer:	https://explorer.getamitycoin.org
Web Wallet:	https:/wallet.getamitycoin.org
Max supply:	100 Billion
Pre-mine:	0%
Emission:	Approx 48m/yr (nearly 200 yr PoW cycle)
Origin:	TurtleCoin fork

Bitcointalk ANN and Social: There is no Bitcointalk ANN and little social media.

Original founders: Amity via public website on Nov 5, 2018 crediting the following original founders of the project: Jack "Mitoshi" James *(Founder);* Aaron "Morpheus" Tomsett *(Co-Founder);* Matt "Hooftly" Hooft *(Project Manager)*; MadHatter *(BotMaster);* Llama.Horse Mining Co. *(Partner).* The project is a fork of TurtleCoin.

Current sponsors: The project is currently sponsored by two pseudonymous community members, @ChrisChaos and @papacabeza.

I. Principles & goals

This pre-white paper outlines our core principles and the goals we want to undertake to make them true for each of the following areas.

A. **Decentralization.** We're part of the movement to maintain decentralized mining.
B. **Community Development.** We're a zero-premine project and depend on the community.
C. **Privacy.** The coin's code is based on privacy and we'll build on that.
D. **Quantum Resistance.** Nothing here yet but quantum is coming.
E. **Collaboration.** We want to collaborate with other projects as much as possible.
F. **Market / Research Division.** Liquidity for miners without spoiling research goals.

With each of the principles in mind, we have set up several goals to advance these principles.

A. Decentralization

Migration to GPU and pool mining. Amity originally launched as a pool-resistant, GPU-resistant coin based on TurtleCoin SoftShell.[1] The algorithm has <u>not</u> proven to be GPU or "pool resistant" as once hoped, and so in the short term (e.g., 2Q19) we will adapt to GPU mining and pools. Later, once stabilized, we will explore options to return to CPU mining.

In our view *decentralization i*s the core principle to maintain rather than any focus (either resisting or embracing). The technologies that best support decentralization currently (from best to worst) are: CPU, GPU, FPGA then ASIC. In the short term, the move to include GPU mining is natural (and may already be occurring in private), so we intend to embrace it. We'll address how we think of further decentralization issues after this next change.

Short term:	Migration to GPU mining
Timing:	1Q19

Long term:	Possible migration to another algorithm (back to CPU, ideally)
Timing:	Unknown

B. Community development

Recruitment. Over the course of the next few months, we want to recruit volunteer community members to join our vision. However "community" means addressing the several requests from the community including mining liquidity (i.e., exchanges). We need coders (so does every project) but we're also looking at this from an interdisciplinary perspective and want contributions from fields of privacy policy, security, regulatory affairs and marketing.

Short term:	Dev -- continued support in regards to the development of the project.
Why:	We are self-taught and still learning and everyone requires help.
Timing:	As long as it takes to find volunteers

Short term:	Community lead, Chinese speaking community
Why:	We want to develop Amity with these users in mind
Timing:	As long as it takes to find a volunteer

Short term:	Community lead, mining liquidity (markets & exchanges).
Why:	Community wants liquidity, but needs to be managed separately.[2]
Timing:	As soon as community lead is identified.

Midterm:	Research Dev -- long term support for areas 3 (privacy) & 4 (quantum)
Why:	Defining the problem is harder than solving for it
Timing:	As long as it takes to find the right volunteers

[1] *See* TurtleCoin, "Introducing CryptoNight Soft Shell," *Medium,* Aug 13, 2018 *available at* https://medium.com/@turtlecoin/introducing-cryptonight-soft-shell-2c2d4c497efd

[2] The distinction between "research" and "market" requires a good sense that any initiative to list and trade a community-based coin like Amity should be led by a separate community-run initiative, and on a separate "market-talk" server.

C. Privacy & Security

Best of class privacy. We're interested in Amity because it's built on core code of a privacy coin. However, privacy as a concept in the crypto space still needs a lot of work and requires the community development of and community education on what privacy means in the context of cryptocurrency. There are tradeoffs in privacy with speed and efficiency, and our intention in this tradeoff will be to optimize for efficiency and speed but not at the expense of privacy. We intend to undertake long-term research in this space in the next couple of years. We also intend to develop the notion of security to mean more than just securing the algo, but the people and systems that host the infrastructure.

Midterm:	Implement Tor and SSL where practical
Why:	Begin to work in well-known best practices to project
Timing:	No time frame as of yet

Midterm:	Privacy researcher(s) from CS and social sciences.
Why:	Set the research agenda for our coin
Timing:	As long as it takes to find the right volunteers

Long term:	Technological research to implement privacy changes
Why:	We anticipate new coding (and a possible hard fork) to make it real
Timing:	As long as it takes for us to get it right

D. Quantum resistance

Address the quantum threat. The quantum computers are coming and anything with a public/private key combination is at risk. We want to get ahead of the curve and find solutions for it. It's longer term. We're watching very closely the January 2019 status report from NIST on post-quantum cryptography.[3]

Midterm:	Dev for quantum resistance
Why:	We need to sort through and choose the best tech
Timing:	No time frame as of yet

5. Collaboration

Our project is the development of many others that preceded it. We intend to be good community participants by inviting collaboration by other projects and by having a collegial, inviting presence on social media.

E. Maintain a firm division between research and market

This is not an investment. Amity is not an ICO and the miners, community members, and participants in our project should have no expectation of any financial return. In fact, as of February 2019 Amity isn't listed on any exchange for crypto and for it to be listed a community member will need to independently sponsor that.

[3] *See* NIST, "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process," NISTIR 8240, Jan 29, 2019, available at https://doi.org/10.6028/NIST.IR.8240

(i) Why list on an exchange at all

Obviously, miners are in this for return, that's what PoW is all about. Miners still want to know "when moon" and when will this coin do amazing things for them financially. We get it. It's not cheap to run rigs and you need to make choices between a project and you want a reward for that. But rewards for work that have a character of a share or stock or investment or something like it triggers rules, including the famous Howie test.

In short, the problem is that other users can acquire the coin on an exchange and come forward to the project thinking they've made an "investment," even though there's no prospectus, no expectation for profit, no intention for any return. Of course, those users can become useful project community contributors (even if they weren't miners), but their character is not as investors, it is as a community participant.

(ii) Formal separation of community/research and market servers

TurtleCoin is perhaps best known for establishing a "no market talk" rule in their main community server. This is an excellent practice and one that we will implement. Concretely, we'll keep the Amity server as-is and convert the OTC server to a market-talk server.

2. Transparency measures

@ChrisChaos and @papacabeza are pseudonymous sponsors and as such, there is already a limit on the kind of transparency that we offer with the project since we're not providing our names and addresses. We intend to take measures to be transparent to the extent that we can within the context of a privacy project, e.g., with a focus on measures that we can provide.

(i) Initial measures

1. Community managed market. So that we maintain our long-term research focus without influence from the "market," and to reduce regulatory concerns, we'll separate our initiatives between c*ommunity/research* and *market*, and embrace the best practice of "no market talk" in the main development Discord. By having a community-managed market we can have a kind of separation of church/state between the purpose of the coin (i.e., R&D) and the needs of the community (i.e., miner liquidity).

2. Lead sponsor wallet (bond) wallet. One of the most important functions for is transparency is that consumers make informed choices. The project's lead sponsors (ChrisChaos@ and papacabeza@) intend to fund a "bond" wallet of 1M AMITY and post the view key for the community to see. These will be personal funds and we intend to see if we can "lock" them in a way that would be similar to a founder, e.g., requiring sales to be notified. (This is a relatively light, initial step and we may take more measures in the future but this is how we're starting).

3. Dev wallet. Additionally, we'll fund and publish a developer wallet to share balances for funds intended for coin development. We'll track spending from the dev wallet in a channel on Discord.

4. No airdrops, no giveaways. Anyone that wants can join the community and rain tips on each other, and sometimes we may do so from our own wallets, but that's just fun and strictly limited to community members: we won't ever have airdrops, giveaways, or anything like that outside our Discord..

(ii) Things that can go wrong

Finally, we hope that via *brutal candor* with our community we avoid many of the risks that occur in the questionable and ever-changing world of crypto regulation. Candor won't inoculate anyone from fraud but it helps to lay out the scenarios when people are making a choice. Is Amity an investment and should you put your future funds in our project and HODL? No, like with any project, community members should be "situationally aware" and skeptical. Here are just a few reasons why.

1. Sponsors not public and sponsorship/management may change. This project started in November 2018 with a published list of founders and sponsors. That has changed a lot since November 2018 and it may continue to change. Moreover, the original project started with people who associated their personal names with it and it is now carried forward by sponsors who are pseudonymous. Although there are other projects in the crypto world with anonymous and pseudonymous sponsors, this doesn't change the fact that you don't really know who is behind the project or what their motivations are; or how those individuals may change over time.

2. Tech is based on open-source contributions by others, unsure of new innovation. Because we can write a white paper it may sound like we're geniuses and have a plan for the future. Truth is that all of our tech so far is based on others and the future innovation is completely uncertain. AmityCoin is a fork of TurtleCoin, which, in turn is a Bytecoin fork, which in turn, is an implementation of CryptoNote. There is a lot of work and a lot of prior art in all these projects (for which we owe gratitude) and we hope to build on this; but the truth is that we may never do anything meaningful and it's possible that the project could just remain stagnant in it's current technology, for better or worse.

3. Scammers probably abound among us. Crypto is rife with scammers.. In our project, we believe in anonymity, and within the community that we develop we may not even know who each other are. This is breeding ground for scams and mistrust. Further, as the community brings us into exchanges the scam-factor could increase because of issues like MapleChange (who would have guessed) or Cryptopia (hacked), etc. It's important for community members to learn "situational awareness" in the full ecosystem, from the community members on Discord all the way through to any exchanges used.

4. This is not a private company, it's a community project. The new sponsors of Amity are excited about the project but Amity is not a profit-generating enterprise and our interest is primarily research based. At times this may mean that your concerns of mining, development, exchanges to be addressed. As such, joining the community will require an understanding for our priority-setting.

After all of this, if you're interested in joining us with Amity, we're happy to have you. We're intending on building the world's most private, quantum resistant, decentralized coin. Please join us!