DIVI Blockchain Development

# Hall Labs Questions & Reponses

January 8, 2018

Responses provided by **CEO Geoff McCabe**

The following responses answers the question regarding the priority importance of focus for Divi Project management.

**1. What are the exact math formulas for how the following is being done?**

DIVI RESPONSE:

The tiers are designated and weighted as follows:

\* Iron: Requires 100 DIVI to be staked

\* Copper: Requires 1,000 DIVI to be staked, offers the baseline staking reward

\* Silver: Requires 3,0000 DIVI to be staked, offers a 5% higher rate of return than Copper, and increases the likelihood of solving a block by 5x.

\* Gold: Requires 10,000 DIVI to be staked, offers a 10% higher rate of return than Copper and increases the likelihood of solving a block by 10x.

\* Platinum: Requires 30,000 DIVI to be staked, offers a 15% higher rate of return than Copper and increases the likelihood of solving a block by 15x.

\* Diamond: Requires 100,000 DIVI to be staked, offers a 20% higher rate of return than Copper and increases the likelihood of solving a block by 20x.

We can imagine three radically different formulas/methods that could all arguably be described this way. Two are simplistic and make the Diamond tier either a) a bad investment and unwise to invest in OR b) a sufficient threat to fail an audit. The third I would NOT have phrased this way (and would still shift the numbers a bit).

**NOTE**: The formulas for the master nodes above are wrong. They should be done in a logical way, in proportion to the amount invested in them. For example, Silver is 3x more likely to earn than a copper + 5% more. So that's why it's better to have one silver than 3 coppers. By the same logic, a Diamond is the same as 100 copper nodes, + 20% better.

**2. Is this formula locked in or can it be changed?**

DIVI RESPONSE: The formula shouldn't be changed. Most of our investors understand the formula and are counting on this, and they've invested specifically to get their Master Node.

There's also a formula that adds on to these levels, based on "vaulting" coins for longer periods of time into the Master Nodes, which means that once they're locked in, they can't be removed, even by the owner. That adds extra stability to the network and also protects the coins from being removed by anyone... hackers, threats, etc. And gives extra rewards. This isn't in the whitepaper but in my Master Nodes, document.

**3. Can it be immediately decided that the fork SHALL be from PIVX?**

DIVI RESPONSE: No I've heard from an expert that although PIVX was forked from Dash a year or so ago, now DASH's code is far superior. PIVX has extra features so the ideal situation might be to fork Dash and add the PIVX features we want, along with our own features.

**4. Can it be immediately decided that the ability for users to write smart contracts shall NOT be required for the Spring deadline?**

DIVI RESPONSE: Yes we think so, we never intended users to write smart contracts. However, some of the features may require smart-contract-like logic for some transactions, such as the vaulting, piggy bank feature, and half-escrow feature (the last one isn't in the WP)

**5. EXACTLY what additional features SHALL be required for the Spring deadline?**

DIVI RESPONSE: We have a list of P0 and P1 features. The most important ones solve the core ease-of-use, security, and fear problems that everyone hates about bitcoin and other cryptos. This list is shown here on the first tab:

<https://docs.google.com/spreadsheets/d/19gB8id8A13_meiL5ACNI--ddJBWOc-6HfZ1oAg1latI/edit?usp=sharing>

Also, the ease-of-use wallet features, many of which don't require blockchain work but are more a matter of smart UX design, are shown here:

<https://docs.google.com/spreadsheets/d/1vR_D-zPaBm9YyA_ql0vQyWQZ1rDJzCA-qYKxST_x22Q/edit?usp=sharing>

My assumption is that we only need to add the necessary API calls to support the new wallet functionality - of which, only the naming functionality is likely to be a technical risk.

That's the most difficult challenge. But, we do have the lead Dev of Namecoin as a consultant to help us, and he's been writing a guide to help us understand how to do this:

<https://docs.google.com/document/d/1blhk5bKOXoOyvAi9bwYJuYgqu7df_I6VdppPJ55BA-A/edit?usp=sharing>

NOTE: It's important to understand that the names part includes a lot of other metadata such as a photo url or two, an email, and some data is public while other is hidden/encrypted.

Another very important feature, which may be a technical risk, is how to send a transfer with a PIN code so that it's done right. It should make the sender and receiver feel far more secure sending money than the current system.

**6. EXACTLY which current PIVX features SHALL be required to be removed for the Spring deadline? In particular, I'm wondering about the Zerocoin privacy protocol that was added to PIVX in October. We could avoid this by grabbing/starting with the immediately prior version of the software. But, is there anything else that we need to immediately disable or remove?**

DIVI RESPONSE: The Zerocoin protocol is probably unnecessary since the previous method is good enough privacy for most situations. But, I'm not sure about hiding balances. Most people aren't going to want their balances to be public knowledge. Also, if we incorporate a strong privacy protocol that has the power to be abused by criminals, then we need to be able to use the governance system to disable it. Or another option is to only allow people to use it who have had their ID verified. Its fairly certain the governments will crack down on cryptos that don't have KYC when serious mass adoption starts to occur.

Another issue about PIVX is that I've been told that the PIVX governance system doesn't work as well as DASH, but this needs to be researched better to confirm it.