

Claim1:

"Blockchain Research Laboratories" is of a coding community ,not an entity.As for the profile of Scott Bingley is authentic.

Claim2:

A working beta product. Accept if: There is a proof of concept of the product on a testnet.

According to the progress,testing main network will be launched in April when the testing data is open.

Open-source code in development. Accept if: There is a significant amount of original code on a public Github repository

Open-source code is going to be opened on Github gradually.Otherwise, the access permission has been opened currently.

Architecture diagrams or novel applications of cryptography and mathematics. Accept if: The whitepaper includes 5 pages describing a novel cryptographic protocol "

At present, the existing encryption algorithms, we carefully compare the implementation of various ECC algorithms in the selection of technology, such as: secp256k1. This algorithm has been actually proved in Bitcoin, Ethereum, EOS and other projects, which already met our the requirements, we are unnecessarily to create a new encryption algorithm.

As for DCC+RDSN, which belongs to the 3 separate parts with the public chain in the technical architecture .In April,the public chain will be launched firstly.Until then,the whole intact data is gonna be produced when 3 parts has been established.

There is nothing showing that SH-DPoS is more efficient and securer than traditional one.

Such a claim needs evidence provided by reproducible tests or previous work from third party.

In traditional DPoS, if a node maliciously issues a block, only the mortgage-related penalties will be imposed, and the corresponding penalties will require human intervention from discovery to implementation. This makes it difficult to ensure the normal processing of the super node group quickly and effectively during this time period, and there are also some malicious block and malicious broadcast verification requirements. **SH-DPos is an optimized DPOS protocol**, which includes a series of automatic repair capabilities for malicious block and error blocks. For example, when a super-node block is verified failure by other nodes, as long as failure blocks reaches a certain number, other nodes will be triggered to initiate a vote removing the node block right, which can avoid performance loss caused by other nodes in the network repeatedly verifying the wrong block information.

The paper appears to be technical but is nothing more than renaming and mixing known technologies in a fashion which is claimed to be feasible and providing utility. The lack of testing, datas, beta and source code can't even partially prove these claims. Thereby there is no novel technology in development. (3.1 of guideline).

We will not create new things which is not to be proved (such as reinventing: tcp/ip protocol,

p2p protocol, cryptography). At present, the emergence of any new products is based on the optimization and combination of existing technologies, created through micro-innovation. we are the same, we are mostly using the existing technology, learning from the current mainstream public chain, we achieve our needs through the optimization of the combination.