

Claims:

Point 2.1. says: “The token issuer’s directors are fit and proper persons (for example they have no previous record of fraud or similar dishonesty offences)”

I claim that the Aurora Chain team shows a first **dishonesty offence** in regard of this court by providing a new whitepaper created **after** the challenge. The only whitepaper from Aurora chain available in public can be downloaded in this address (the one from the website):

<https://www.aurorachain.io/Aurora%20Chain%20white%20paper%20EN.pdf>. Jurors can see that the metadata of this document (using adobe pdf File>Properties) shows a creation date of 2018/09/04 (yyyy/mm/dd) which is before my challenge (2019/07/16)

After the challenge began Aurora team shows some evidences linking another whitepaper in this address: https://www.aurorachain.io/pdf/AuroraChain_White_Paper.pdf. Metadata shows a creation date of 2019/07/17, one day **after** the challenge.

Jurors should quickly verify this before any attempt of removing these evidences occurs.

This is totally unfair to consider a paper that the challenger can’t had have access before the challenge. Evidences in favor of the challenger can be removed and nullify claims, destroying incentives to challenge in the first place.

This claim only is sufficient to deny the badge, ethfinex guidelines mentions precisely “dishonesty offences”.

At least please consider this move as not fair and hostile for your ruling.

From now any reference to the Aurora whitepaper mentions the one I had access to
<https://www.aurorachain.io/Aurora%20Chain%20white%20paper%20EN.pdf>

Point 3.1, about “Technology and Product” is not fulfilled by the challengers token.

Point 3.1 says: “There must be evidence of novel technology in development”

I have to share how I understand ‘novel technology’ when reading 3.1.1, 3.1.2, 3.1.3. For example, having a working beta product means having a working beta product **related to the goal of the project and with evidence of novel technology used for that**. Otherwise the founders could just publish a basic Qt wallet, or even a text editor program (or anything totally unrelated) to fulfill this requirement. The same reasoning with the open-source code apply(the guideline emphasize it with ‘significant amount of original code’).

Apps and deployed programs

I’ve tried the windows mainnet wallet and didn’t find anything that others like Komodo did ages ago. Very basic stuff. Deploying contract and assets, sending/receiving token, voting in a DPOS environment, that’s all.

The mobile application on android contains “Dapps”, mainly gambling games. We can see 26 ‘Dapps’ when in reality Aurora block explorer shows only 8 contracts deployed :

<https://browser.aurorachain.io/contract.html#/> In my understanding a Dapp is an application using a smart contract in back end. How can we get 26 Dapps with only 8 contracts deployed?
Sophisticated use of smart contracts resulting in a useful product for industries could have been ok to

fulfill the requirement, I guess. But nothing of interest was found in the contracts code. Check for yourself it's simple code, mainly gambling games, vote system, token generation.

Code

<https://github.com/aoaio/go-aoa> shows only standard technology for running wallet, blockchain client, deploy contracts, deploy assets, etc... Nothing new. It's a copycat of Ethereum blockchain with DPOS, which exists already.

Now, founders will probably argue back showing some codes saying it's original. Right, they renamed functions, maybe change some variables, assembled code and ideas from other projects and call it new stuff. But look for yourself, you will not see anything special. To give us some clues of what can be worth a look in the code maybe we should look at the whitepaper. After all it's where is presented new technology serving unique purpose.

Whitepaper

I focused on chapter three which describe technical realization of Aurora Chain objectives

DPOS+BFT

This is something promised by bitshares and EOS : <https://www.youtube.com/watch?v=Xs1dyZFhlr4> but they have not implemented it yet <https://github.com/bitshares/bitshares-core/projects/15#card-17426735> (bitshares)(last item in To do list) <https://github.com/EOSIO/eos/issues/2192> (for EOS)

Can requester shows us how it implemented it knowing multi billion dollars projects failed to deliver it?

Smart contract

They say they will use smart contracts.

P2P stereo net

"A broadcasting network is built among different nodes. Proxy candidates can build up direct connection through the upper layer network which enables that BFT mechanism between proxies could be realized quickly. With network layering, we can achieve faster and safer communication."

I simply don't understand what it means. The BFT DPOS part gives us more :

"Aurora Chain builds up a stereoscopic P2P network where there is a broadcasting network among nodes based on UDP and a long connection among proxy candidates based on TCP. Through the upper network, a high-speed BFT consensus system can also be realized among proxy candidates"

Well, Bitcoin can use UDP broadcasting with FIBRE protocol. It's just not as reliable as TCP, but speed is increased. We can't seriously think using TCP or UDP as a new thing. It's really in public domain, and common knowledge among computer engineers.

Intelligent application isolation technology

"Verified transactions will be processed in the Pending Zone. Proxy nodes pack transactions in the Pending Zone until let out. Major functions of the smart scheduling pending area are as follows: 1. From a macroscopic view, it distinguishes contracts with different fees, flows and categories. It also takes a dynamic control of transaction's entering the Blockchain to make sure the process is fair and that clog of some contracts won't affect others. 2. From a microscopic view, it can monitor each contract in real time and make adjustments according to the real situation. It makes Blockchain more

efficient and protects it from outside attacks." I suppose this 'new' technology https://github.com/aoaio/go-aoa/blob/master/core/tx_pool.go refers to transaction pool we have in Ethereum https://github.com/multi-geth/multi-geth/blob/master/core/tx_pool.go. It's all I saw related to this in the code. Requester could show us which code to look at. What's given in the whitepaper doesn't give us means. Claims about efficiency are unbacked until proven.

Multi-asset offering

"Procedure of asset offering can be simplified, with provision of processing speed and capability of expansion with the same level as main chain coins. The standard token offering procedure offers includes simplified and regulated token offering methods and procedures. With multi-asset token offerings, tokens can be used in the contracts directly and there is no need for introduction of other contracts. »

Very hard to understand what is proposed here. I think it's the fact that it's possible to emit a token on the Aurora Chain using a contract like ERC20. (I think I found this contract on the explorer) Komodo did it.

The multi-chain parallel technology

"The multi-chain structure makes transaction process more efficient than the single-chain structure for the latter is restricted by encryption algorithms and online transmissions. The stereoscopic P2P network can realize a cross-chain consensus system and increase TPS. Therefore, the ability of Blockchain can be infinitely increased as the number of chains increases"

Unbacked claims mostly, multi-chain exists and run with Komodo

<https://komodoplatform.com/komodo-platform-new-scalability-solution/> I don't see why their stereoscopic P2P network specially help for that

The upgradable Blockchain

"It's hard to upgrade Blockchain after it has been released except when a compulsory fork is applied at the expense of impeding the development of Blockchain. But with the LLVM compiler, Blockchain code and contract scripts will be put together. All clients will upgrade together after the upgraded Blockchain is placed on the old version at a specific link."

"Aurora Chain commits itself in building upgradable blockchain and realizing automatic upgrading in designated height". So Aurora Chain is able to fork automatically at some block height. Which means the governance is centralized? Founders are able to push new code and fork their blockchain automatically.

The main problem with this whitepaper is that a lot of technical "solutions" supposed to answer a problem are way too vague, and use unnecessary complex expressions or words to make it "technical" Anyway, upgrade decided by voting process of the holders are implemented in Tezos and EOS.

Cluster self-grouping

This thing is interesting but still in research domain (<https://arxiv.org/pdf/1902.02174.pdf>) I don't know any implementation and I can't find it on the Aurora github. The mechanism is not described enough in the whitepaper (in comparison, the link above do what's real research, and prove developing of new technology) No academic research is provided by Aurora team.

The anti-quantum-attack technology

They say they will apply lattice-based cryptography. It's still in research domain and there is no one who deployed that in crypto. I don't see any PHD in the team capable of addressing this highly technical expertise which is quantum cryptography. Everybody can say that, which signatures system based on lattice ?, need details ! (I can't believe they can produce this stuff from scratch)

The cross-chain communications

"Currently, it's still impossible for block chains are to communicate with each other. The isolation prevents different block chains from working together and impedes their development. Aurora Chain, however, supports a cross-chain communication protocol and other crosschain technologies to ensure an unrestricted value-network"

Look at what Komodo did in the domain.

The differentiated mining mechanism

"On the Bitcoin network, mining nodes pack transaction records independently into new blocks through the workload management approach and get Bitcoins as a reward. The core of mining is to reward community members according to their contributions and therefore to encourage their participation. Aurora Chain gives rewards to anything making contributions to the community such as upgrading the code, finding bugs, giving optimizing suggestions and spreading knowledge as long as they are recognized by the community members. The mining system won't be written into the Blockchain in the beginning. Instead, it will be tested and optimized in the community until the rules are finalized to maximize incentives."

They describe discretionary reward of community members based on subjective and not linked to cyberspace notions like: "spreading knowledge" or "giving optimizing suggestions". Of course, it has to be centralized. It's subjective or too complex to model an incentive system based on that.

That's all for the technical part of the whitepaper.

Conclusion:

Point 3.1 speaks about "evidences" of novel technology and shows us three way to find them.

- Deployed apps or product shows proof of concept of a new technology used to fulfill objectives of the project. In our case, having try desktop and mobile apps, even 'Dapps', there is nothing of interest and which differentiate this project from what we have seen in the space since years. Work has been done, but only what is crucial to deploy ERC20, explorer, deploy contract, etc.... Try it and ask yourself regarding the objective of the project:
 - o Can it help incorporating Blockchain into other industries?
 - o Does it leverage new technology for that or try to ? which one ? is it novelty, or something 100 tokens already used ?

If the answer is no, it's ok, we have others ways to find evidence, maybe using the apps doesn't shows it, backend is maybe what's interesting, or may be new stuff is simply not implemented yet but under development. That's why we look at the code

- Source-code gives opportunity to people to see new stuff in development, encourages contributors to participate, discuss it. The Aurora github has no activity showing some interest from community, no issues, pull request, only 4 contributors. The main code is another melting-pot of other projects. And that's ok to not reinventing the wheel, but it needs original ideas and I didn't find one. I tried my best to search in the repository some

hint of new stuff explained on the whitepaper. Load balancing among clustered nodes ? Ok let's check it out..... Nothing. Maybe I didn't find it, after all there is too much code to verify everything, so I ask requester to shows us some code about describing cluster self-grouping technology? automatic upgrade? intelligent application isolation technology? Or any feature you describe as new, to see what's really there.

So nothing new in the implementation level, but it's alright, new technology need specifications, theory, deep explanation. So let's check resources, is there academic work ? no, just a whitepaper. It's ok, satoshis whitepaper was enough to explain everything.

- The whitepaper should give us in an understandable manner, what technology the team intends to use for realizing their objectives. If deployed program or codes failed to give us hints of novelty, the whitepaper could be enough, provided that it has some technical substance. For Aurora the answer is definitely no. And it's too easy to just write some fancy names and features. If one feature can be demonstrated with the apps, or visualized within the code, it's ok if the whitepaper is not very specific. But if we have neither, whitepaper have to be specific, otherwise it's just unbacked claims, we can't **verify evidences**.

I hope my point of view will be shared by jurors, and that they will not be fooled by some code and mobile app which everyone can do with minimum skills. Otherwise it means it's really easy to game this badge.