# Aurora Evidence

First of all, we are very grateful to Challenger for devoting attention to, and raising important questions about the Aurora project. We will respond to the Challenger's concerns.

Let us initially explain our understanding of blockchain technologies.

First, blockchain is not a new technology. Blockchain is a new application model that uses existing computer technologies such as distributed storage, peer-to-peer transmission, consensus mechanisms, and encryption algorithms. It is essentially a decentralized database, an underlying technology that is a string of data stored and secured with cryptographic methods.

Second, blockchain is an idea. In addition to representing a technological innovation, the theoretical innovation of blockchain technology is a greater revolution. The decentralization, openness, independence, security, and anonymity of blockchain technology grants all people and organizations a fair way to engage in social and economic transactions. In short, blockchain democratizes participation on the internet.

Third, the vision of the AOA Aurora Chain is to leverage blockchain technology to build a broad-based ecological solution. We are not going to be Bitcoin, and we do not seek to become or compete with Ethereum or Komodo -- the projects the Challenger repeatedly mentions. The blockchain field is inclusive and open to a multiplicity of ideas and approaches.

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

**Explanation:**

The Aurora Chain has now completed all development work on the upgradeable blockchain, as detailed in Github. We are constantly updating the brand, the code, and the white paper.

With respect to the pace of development, and because this is systematic, incremental work, we update the white paper as additions to the core are confirmed.

After submitting the Badge application, to better explain the progress of the project to the jurors and Challengers, we immediately submitted multiple, comprehensive materials, including the latest version of the white paper, all in good faith. Please note that the Challenger did not submit evidence in a timely fashion. The deadline for submitting full materials was 17 Jul 2019 16:55:40 GMT, but the Challenger did not submit evidence until 19 Jul 2019 14:58:16 GMT. That we followed normal, proper procedure and protocol should be enough to prove that we did not alter our materials or otherwise engage in dishonest behavior according to the allegations of the challenge. As according to our plan, our brand upgrade and the latest version of the white paper update will be completed in August, we just synchronized the relevant information to the badge application in advance.

The development of emerging technology projects obviously follow a roadmap for introducing innovative tools and products. Some information needs to be kept confidential and cannot be released to the public. In this context, we decided to add relevant information that would otherwise have been withheld to materials submitted. As for the review rules regarding new or old white papers, this can be decided by the jurors.

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.

**Explanation:**

First, we need to clarify the terms of 3.1, Point 3.1 suggests: "There must be evidence of novel technology in development". Please note that the phrasing used is "in development." This means that development is ongoing, in progress, and that it need not yet be implemented. By including forward-looking statements in the whitepaper, we invite collaboration and competition.

Second, the broad goal of the genre of the white paper, that is to say any white paper, is to present both a technical vision and practical solutions to problems that users face. We are working towards the goals laid out in our white paper: we have completed the first phase of development, but the development of the second and third phases is still in progress.

Third, regarding the APP issue and the comparison with Komodo, we are unsure if the Challenger is referring to IDE development tools. The Smart Contract IDE is provided by a third-party partner at the following address: http://solc-aoa.egretia.io/. Our main network integrates the Egret game development platform tool, which makes deploying game apps both time and cost-efficient. It is true that we show 8 contracts on our browser. But there are in total 26 DAPPS whose developers have reached strategic cooperation agreements with Egret game providers such as Aurora. These developers will release their games in batches, and products will be tested and configured in advance. As they are prepared for release, DAPPS will necessarily be displayed on the APP homepage in advance, but access will only be opened to users once the configuration is completed. The Challenger suggests that smart contract applications can solve many problems, and that there is a need to explore industry solutions. But the functions provided by smart contracts are very limited. There are many ways to combine DAPP and blockchain, and in many cases, smart contracts are not even necessary. Must one force users to write a version of World of Warcraft using smart contracts? This is unrealistic. We just provide a platform, leaving it to game developers the choice of how they want to use the blockchain -- with smart contracts or without -- to provide users with the perfect experience.

Fourth, blockchain is not just a technology. The idea of cryptography and decentralization is a design idea. If you learn from it, the Ethereum code is as much a reference as a solution. Ethereum itself uses the encryption method of Bitcoin and draws on the *C++ lib* library. At the outset of the project, we drew inspiration from powerful and mature blockchain implementations. Since then, we have sought to improve and even rework the technology according to our own blockchain design concept.

Fifth, regarding the code problem, the Challenger argues that there is nothing innovative in our code base. Everyone has a different understanding of products and technologies, and each person's technical background is different. The Challenger's subjective opinion that there is nothing original should not be taken as an objective fact. We hold that the Challenger's subjective claim completely negates the achievements of developers and technicians who have worked day and night on the platform.

At present, AOA has completed phased development work on the upgradeable blockchain and consensus mechanism; this content is original. We will continue to update and improve, as we follow our technology roadmap.
Https://github.com/aoaio/aoa-upgrade
Https://github.com/aoaio/go-aoa

We invite the jurors to evaluate the code.

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=Xs1dyZFhIr4 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?

**Explanation**

First, we must explain that we understand the DPOS and BFT consensus mechanisms as macro concepts, in other words, as design ideas that do not represent a specific implementation solution. We are following our own design and methodology in the final implementation of these mechanisms.

Just as EOS and Bitshare follow their own design, AOA is driven by a specific vision that guides development. We encourage you to visit our Github repository and to review our code.

Third, we believe that in the blockchain landscape, every project that strives to innovate merits respect. Not all innovations emerge from projects as well-funded as EOS.

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.

**Explanation:**

First, TCP and UDP are common network communication protocols.
Second, our focus is on network layering, not TCP and UDP. What we will achieve is two-dimensional communication whereby the proxy node is separated from the common node in the consensus process. Our design solves the limitations of time-consuming forwarding and searching that takes place in only one dimension.

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 shows us which code to look at. What’s given in the whitepaper doesn’t give us means. Claims about efficiency are unbacked until proven.

**Explanation:**

What we call the intelligent isolation zone is a big solution that solves many practical problems, such as the congestion on Ethereum caused by the CryptoKitties traffic. Intelligent isolation is our key offering, and the solution is at the core of all three stages of our development roadmap. In the current stage, we implemented a part of the analysis and dynamic balance of all transactions. For example, when the transaction volumes on smart contracts are very large, one finds across the board that processes across a blockchain are slowed. Our solution is to find ways to batch process transactions on the same contract. This radically improves efficiency and user experience. We offer a concrete solution to problems that users repeatedly encounter.

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.

**Explanation:**

First, the Challenger may not have experienced the pain of having backdoor entries implanted when writing ERC20 code -- resulting in the theft of tokens traded on an exchange. He may not have experienced the pain of ERC20 participating in FOMO3d, or the pain of the person who wants to distribute tokens and who needs to enter the fee for each address. We seek to solve these pains via mechanisms that allow simple, standardized, and secure collection of funds that does not require expensive payments to complete the Token function of code security auditing.

Secondly, our aim is to solve the problems that plague non-technical or “newbie” users. We do this in part through multiple assets (and primary and sub-addresses). Is this useless?

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

**Explanation:**

We have a multi-chain solution in development. The Aurora team is responsible and cautious, and we will not publish solutions until our code is finalized and fully tested. Good development takes

time, and we believe that in the open and inclusive field of blockchain, our offerings will have tremendous impact.

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.

**Explanation:**

We are not centralized, and our chains upgrade through community voting. The entire, streamlined process is as follows: First, the proposer submits an application to upgrade to the new version.
Second, the new version must be approved and voted in by the community.
Third, after the vote is passed, all users' clients will automatically upgrade at a fixed block height.
Blockchain upgrades are not so easy to implement -- take for example the fork of Ethereum Classic and Ethereum. Our upgradeable solution relies on fairness, community voting, and transparency.
We are focused on practice, and our solutions will speak for themselves, more than the white paper.

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)

**Explanation**

This is our technical vision to solve big data problems. Due to limited time and energy, we have elected to focus on the upgradeable blockchain and consensus mechanism in the current, early stage of our work. We believe that each project takes time to grow.

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.

**Explanation:**

We are not familiar with Komodo, but we did learn and draw early on from the now mainstream ideas proposed by Cosmos and Boca. One cannot build behind closed doors, and we freely admit to taking inspiration from cutting-edge, advanced blockchain theory.

The consensus mechanisms of AOA and Bitcoin are different, because AOA does not need mining. What the plaintiff mentions -- “spreading knowledge” or “giving optimization suggestions” -- fall under the domain of our decentralized community reward system that is overseen and paid for by the foundation. Our idea is to include the community in deciding both the recipients and awards for contributions to the platform.

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:

- Can it help incorporating Blockchain into other industries?
- 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.

Explanation

First, our goal is to serve users. The blockchain platform we provide is open to everyone, and we do not seek to control specific development contracts implemented by users.

Second, in all fairness, applications across the blockchain industry remain at the exploratory stage. At present, we believe that there are no APPs with special qualities or disruptive models. We should allow apps the space and time to mature..

Third, the blockchain support scenarios that can be seen in other industries are now reflected in our platform, and they have all been optimized. Others aim at similar solutions.

Fourth, our project is practical and pragmatic. We are focusing on the solutions that we actually encounter in our application areas. Many blockchain macro concepts are common to all projects, but the specific solutions are different. For example, all projects mention consensus mechanisms, but each project implements a different solution. Innovation occurs at the level of implementation and application, not at the surface-level. Cryptography is another example of a common concept that everyone uses, creating new solutions through the classic technology to serve the public.

Fifth, regarding the Challenger's problem, this has something to do with our development model. Most of our development is concentrated on the Gitlab internal library, and Github code submission is also done by a fixed staff. Because we have many solutions, we conduct many trials. Some of them fail to be deleted immediately, so the final presentation is only our staged submission. If you want to see original ideas, we have implemented a consensus mechanism and an upgradeable function.

**Conclusion:**

First, we hope to impress on the Challenger that macro-blockchain concepts and specific solutions are two very different things..

Second, each person's technical background is different, and each understanding or reading of the code is different. You cannot ignore the labor results of others because you have not found it. We implore the jurors to closely examine the upgradeable-blockchain and consensus mechanism portions of our code, which are implemented and completely original.

Https://github.com/aoaio/aoa-upgrade
Https://github.com/aoaio/go-aoa

Third, we hope that blockchain can be a space of plurality, where multiple voices contribute. The landscape should not only be dominated by projects like EOS. Please recognize that we are a developing project motivated by big ideas and the desire to have significant impact.

Fourth, the author repeatedly mentions Komodo, with which we are not familiar. We do not rule out that there may be overlaps in the concept, but the solutions are different. Our approach and design is unique.

We hope that the above serves to help jurors develop a comprehensive understanding of the Aurora Chain  project.