

The Baer Chain is not compliant with Ethfinex guidelines

Context:

Ethfinex proposes a badge to tokens who comply with a set of guidelines published here : <https://ipfs.kleros.io/ipfs/QmVzwEBpGsbFY3UgyjA3SxgGXx3r5gFGynNpaoXkp6jenu/Ethfinex%20Court%20Policy.pdf>.

Claims:

Claim 1

I claim that point 2.1 among guidelines is not fulfilled, thereby, Crypto.com Chain can't be granted with the Ethfinex badge.

Claim 2

I claim that point 3.1 among guidelines is not fulfilled, thereby, Crypto.com Chain can't be granted with the Ethfinex badge.

Evidences:

Claim 1

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

You can find the details about the team of the issuer on his webpage :

<https://www.baerchain.com/site/team>

I took attention on the profile of the CTO named Scott Bingley. At the date of 03/22/2019, it says:

“Bachelor of Information Software Engineering, University of Chicago, Master of Software Engineering, University of Boston. He owns 15 years of software development experience, used to work in Cisco and Motorola as the chief technology engineer, participating in leading the systematic framework design, research and development of multiple major projects. Scott has significant mathematical, logical and data analyzing abilities, and grasps software development technology of state-of-art around the globe. He was the senior researcher of Blockchain Research Laboratories in Oxford and IBM, and has deeply studied cryptography and distributed storage, etc.”

have more than 10 years working experience in game creation and development. Worked in Hongkong Run Up Game and Korean NEOWIZ as senior executives successively, and guided department members to finish prototype design and creation of game characters. In 2015, established GogiiGames in Hongkong and developed the game Xjingzhi independently, which was purchased by Tencent later. In 2016, he started to concern block chain technology. Co-founder of Hongkong Baer Tech.



Scott Bingley Baer Chain CTO >>>

Bachelor of Information Software Engineering, University of Chicago, Master of Software Engineering, University of Boston. He owns 15 years of software development experience, used to work in Cisco and Motorola as the chief technology engineer, participating in leading the systematic framework design, research and development of multiple major projects. Scott has significant mathematical, logical and data analyzing abilities, and grasps software development technology of state-of-art around the globe. He was the senior researcher of Blockchain Research Laboratories in Oxford and IBM, and has deeply studied cryptography and distributed storage, etc.

The final statement about being a senior researcher of Blockchain Research Laboratories in Oxford is not consistent with the facts following:

- There is no entity called “Blockchain Research Laboratories” in Oxford
- I contacted the director of the closest entity by name called “Blockchain Research Center” and this person is not known there <https://blockchain.univ.ox.ac.uk/> (Mail of the director : awroscoe@gmail.com)
- There is no scientific publication written by Scott Bingley neither we can find his name mentioned as a contributor on the topic of “blockchain” or “cryptocurrency”. It’s highly unlikely for a senior research scientist.
(https://scholar.google.fr/scholar?hl=fr&as_sdt=0%2C5&q=scott+bingley+blockchain&btnG=)

One of the founders and CEOs named Ziv, doesn’t have any public profile, which makes hard any due diligence. Not having any public profile remove the ability to verify point 2.1 completely and should be considered by the jury as a red flag.

These facts form a body of corroborating evidences that makes possible to establish dishonesty of the issuer about the team.

Claim 2

Point 3.1 about “Technology and Product” states:

“There must be evidence of novel technology in development. This may be evaluated for example by demonstrating: (Only one stipulation is required)

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

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

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

Whitepaper study

We base our assertions on the whitepaper provided by the issuer:

https://www.baerchain.com/statics/BaerChainWhitePaperv1_2.pdf

The whole whitepaper is a mix of

- 1) Obvious statements about known technologies like this one about cryptography

“The core of digital encryption is cryptography. Encryption is the process of converting plaintext into ciphertext by encryption algorithm and encryption key, while decryption is to restore ciphertext to plaintext by decryption algorithm and decryption key.” And this one about multi-signature *“Each account can be controlled by any weighted combination of other accounts and private keys. This mechanism creates a hierarchical privilege structure that can truly reflect the organizational situation of authorities in reality and makes it easier than ever for multiple users to control funds.”*(5.2 DF)

Or this one about block structure:

“In the Baer Chain technology scheme, the data structure is divided into header and body. The header includes the hash that links to the previous black. It assures the basis of chain data irreversible by using time stamp, random number, body content and the hash of the previous black, etc. The body records the complete packed transaction information. It uses public prefix to compress the character string via Merkle-Patricia-Tree, for the purpose of improving inquiring efficiency and saving storage space.” (5.1 SH-DPoS)

- 2) Unbacked claims like :

“At the same time, this kind of structure assures that when malicious blacks appear, not only the blacks labelled as Cancer will be mitigated to guarantee the security of the whole public chain, but also the useful information in Cancer used, promoting the speed of generating blocks after meeting malicious blocks. Therefore, when meeting malicious blocks, the SH-DPoS is more efficient and securer than the traditional one, assuring the high-efficiency of error-correction, fast delivery and strict protection of values from the underlying logics.” (5.1 SH-DPoS)

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.

“The redundant storage of RDSN meets the requirement of efficiency and stability with DCC, while the security of the whole resource storage is accomplished by SBSC.”

Again, no data proves this claim.

3) Renaming of known technologies with obscure acronyms

RDSN for “Redundancy Distributed Storage Network” (I only found the meaning of this acronym in their medium page : <https://medium.com/@singaporebaerchain/redundancy-distributed-storage-network-rdsn-80577cd17b57>, **I urge the jury to read this article which should reveals a red flag.**) is nothing more than a distributed hash table (https://en.wikipedia.org/wiki/Distributed_hash_table)

The SBSC for “Static Business Ressource Summary Chain” is adding redundancy to the distributed hash table system by putting data in blocks which is a highly inefficient way of adding redundancy.

Github

The github repository of the issuer is not published on their website, I had to use Google, it’s not very convenient for someone willing to work on an open-source project. The github seems to be this one: <https://github.com/BaerChain>

I found that there is no public member to the project and almost no original code. Only code for the wallet of the ERC-20 token has been committed. There is no activity since November 2018.

There is simply nothing to review about. No code, no testnet, no mainnet, no MVP, no beta, only a wallet is published on the website.

Conclusion

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).**