IEEE P3209

Standard for Blockchain Identity Key Management

January 28, 2021 UTC+8

Online, China

1. Call to Order
* All the people introduce and announced their identities.
1. Approval of Agenda

• the chairman introduces the agenda

* Motion # 1

Moved: Xianping Mao Ontology Foundation Ltd

Seconded: Chao An [Mathtech Co., Ltd.](http://www.mathtech.com.cn/)

Motion passed by voice vote without opposition

1. Review and Approval of Last Meeting Minutes
* Review last meeting minutes

• Motion # 2

Moved: Mimi Deng Sichuan Changhong

Seconded: Han Chen Huochain Technology

Motion passed by voice vote without opposition

1. Working Group Membership
* The sheet has recorded the participants.

|  |  |  |
| --- | --- | --- |
| Yu Lang | Bytom Foundation Ltd. | Chair |
| Qiufeng liu | Bytom Foundation Ltd. |  |
| XiangZhou Shen | Bytom Foundation Ltd. |  |
| Wenqi Zhao | Huochain Technology | DR |
| Han Chen | Huochain Technology | DR |
| MiaoYan Xu | Huochain Technology | DR |
| Jingzhi Zhang | China Zheshang Bank Co., Ltd. | DR |
| Haihan Zhou | Beijing gongyilian Technology Co., Ltd | DR |
| Jiajia Liu | IEEE | Staff |
| Meng Zhao | IEEE | Staff |
| Xiaofeng Chen | Hangzhou Qulian Technology Co., Ltd. | DR |
| YiJian Zhang | Hangzhou Qulian Technology Co., Ltd. | DR |
| Chao An | [Mathtech Co., Ltd.](http://www.mathtech.com.cn/) | DR |
| Yingying Jiao | Hangzhou Yunphant Network Technology Co. ,Ltd. | DRA |
| Jiren Ma | Shengjian Network Technology Co. ,Ltd. | DR |
| Mimi Deng | Sichuan Changhong | DR |
| Xianping Mao | Ontology Foundation Ltd | DR |
| Yufeng xi | Sensetime Technology Co. ,Ltd. | Observer |
| XiangJuan Jia | Zhejiang University | DR |

1. Call for IEEE Patent Policy
* The chairman introduced IEEE patent policy
* No potential basic patent requirements have been announced and no potential basic patent holders have been identified
1. Call for IEEE Copyright Policy
* The chairman introduced IEEE copyright policy
* No potential basic Copyright requirements have been announced and no potential basic Copyright holders have been identified
1. Presentations
* Qiushan Liu Bytom introduced the draft of the Standard for Blockchain Identity Key Management including the rules of seed and hierarchical deterministic derivation, and the rules for generating seeds according to mnemonic words, and hierarchical path specification, and the keystore schedule, and the cross-chain authentication schemes.
1. Discussion
* Haihan Zhou Beijing gongyilian Technology Co., Ltd,asked that if the stored key strength is too weak, it will lead to key cracking, how to avoid it. Dr. Mao Ontology Foundation Ltd answered that we should follow specific rules when choosing passwords to avoid weak password problem.
* Xianping Mao, Ontology Foundation Ltd, thought since the address generation algorithm and signature algorithm are different in different blockchains, if the standard is not clear about the relevant algorithm involved in the scheme, it will lead to the problem with the solution. Qiufeng Liu indicated that they would follow the suggestion.
* Wenqi Zhao Huochain Technology，concerned about whether If the parent private key is compromised, whether the child private key is also insecure. Qiufeng Liu answered that the Standard will avoid this problem by the strengthening derivation rules.
* Han Chen Huochain Technology，asked the difference in strength between cross-chain derivation and no cross-chain derivation.
* Qiufeng Liu answered that hierarchical derivation is independent of cross-chain authentication.
1. Future Meeting

• Next group meeting is scheduled for February 28th

1. Adjourn

• Motion # 3

Moved: Chao An [Mathtech Co., Ltd.](http://www.mathtech.com.cn/)

Seconded: Yingying Jiao Hangzhou Yunphant Network Technology Co. ,Ltd.

Motion passed by voice vote without opposition

15：05 Adjourn