IEEE P3209

Standard for Blockchain Identity Key Management

June 24, 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:Ping Lu Fuyun Network Technology Co., Ltd.

Seconded: Xianping Mao Ontology Foundation Ltd

Motion passed by voice vote without opposition

1. Review and Approval of Last Meeting Minutes

* Review last agenda

• Motion # 2

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. Working Group Membership

* The sheet has recorded the participants.

|  |  |  |
| --- | --- | --- |
| Yu Lang | Bytom Foundation Ltd. | Chair |
| Qiushan liu | Bytom Foundation Ltd. |  |
| XiangZhou Shen | Bytom Foundation Ltd. |  |
| Han Chen | Huochain Technology | DR |
| Jinzhi Zhang | China Zheshang Bank Co., Ltd. | DR |
| Mengwei Han | Zhejiang University | DR |
| XiangJuan Jia | Hyperchain Co., Ltd. | DR |
| Chao An | [Mathtech Co., Ltd.](http://www.mathtech.com.cn/) | DR |
| Jiren Ma | Shengjian Network Technology Co. ,Ltd. | DR |
| Yinyin jiao | Hangzhou Yunphant Network Technology Co. ,Ltd. | DR |
| Mimi Deng | Sichuan Changhong | DR |
| Hongjuan Kang | Sichuan Changhong | DR |
| Jian Zhang | Sichuan Changhong |  |
| Xianping Mao | Ontology Foundation Ltd | DR |
| Ping Lu | Fuyun Network Co., Ltd. | DR |
| Jiajia Liu | IEEE | Staff |

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

* Han Chen Huochain Technology reported the details of random number generation, grouping, mnemonic word generation and seed generation. At the same time, several problems need to be discussed are put forward.As follows:

Select true random standard or pseudo random standard when initial ENT is generated？

Whether self-built thesaurus should be required to be open？

How to check the security of the self-built thesaurus if small languages are selected？

Whether the implementation and standards of smart contract wallets need to be considered？

* Mimi Deng Sichuan Changhong introduced three kinds of key derivation functions, suggested the improvement scheme of keystore, and suggested another method of cross-chain self-authentication.

1. Disscussion

* After discussion, experts believed that there is no safety standard for true random algorithm and pseudo-random algorithm should be adopted.
* As for the key derivation algorithm, Xianping Mao, Ontology Foundation Ltd, thought that the key derivation algorithm should not be specified, and only the security specification requirements that the key derivation algorithm needs to meet should be specified in the standard.
* Experts believed that cross-chain self-authentication scheme exists the risk of leakage. Zhang Jian Sichuan Changhong proposed to add a timestamp when using signed address to prevent the risk of leakage of signed address.
* Xiangjuan Jia thought that the structure and content of the standard need to be adjusted, and the chairman said that they will improve it in the next draft.

1. Future Meeting

• Next group meeting is scheduled for July 24th

1. Adjourn

• Motion # 3

Moved: Mimi Deng Sichuan Changhong

Seconded: Mengwei Han Zhejiang University Co. ,Ltd.

Motion passed by voice vote without opposition

16：00 Adjourn