IEEE P3209

Standard for Blockchain Identity Key Management

April 29, 2021 UTC+8

SUZHOU, 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: 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 agenda

• Motion # 2

Moved: Yijian Zhang Hyperchain

Seconded: Jinwen Fan Sichaun Changhong

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 |
| Jiajun Chen | China Zheshang Bank Co., Ltd. | DR |
| Yijian Zhang | Hangzhou Hyperchain Technology Co., Ltd. | DR |
| Chao An | [Mathtech Co., Ltd.](http://www.mathtech.com.cn/) | DR |
| ChunFeng Luo | Hangzhou Yunphant Network Technology Co. ,Ltd. | DR |
| Tianbu Huang | Hangzhou Yunphant Network Technology Co. ,Ltd. | DR |
| Mimi Deng | Sichuan Changhong | DR |
| Jinwen Fan | Sichuan Changhong | DR |
| Xianping Mao | Ontology Foundation Ltd | DR |
| Dan Zhou | TeSilian Technology Co. ,Ltd. |  |
| Lin Hao | NAST |  |
| Yi Meng | Haier | DR |
| Ping Lu | Fuyun Network Co., Ltd. | 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 reviewed the goal of the Standard for Blockchain Identity Key Management at first,then 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.
* Qiushan Liu Bytom showed the problems left over from the last meeting as follows:

In the section of seeds,in addition to the 12 words,should there be other methods.

When use the private key to derive the public key of the same level,which digital signature algorithm to choose,secp256k1 or other Edward Eliptic Curve?

About CKD/HKD,only recommend sha512?

About Cross-chain:

Whether to add a time period, regularly check compatibility with some target chains(such as fork)?

should we add some kind of privacy protection mechanism to let Users choose whether their public key can be discovered autonomously?

Under the same account, the user has the habit of changing the public key every time after completing the operation, is it still possible to smoothly complete cross-chain self-certification?

1. Disscussion

* Xianping Mao, Ontology Foundation Ltd, suggested the algotithm involved should not be too detail.He thought the standard should be a framework. Qiufeng Liu indicated that they would follow the suggestion.
* Xianping Mao, Ontology Foundation Ltd thought that if the keystore is used for a long time, the keystore can be leaked. Qiufeng Liu said they would consider the risk and reduce risk as much as possible.
* Jinwen Fan thougth the difficulty level of the CKD/HKD should be suggested.
* Qiushan Liu divided the standard into five parts,including the rules of seed and hierarchical deterministic derivation, the rules for generating seeds according to mnemonic words, hierarchical path specification, the keystore schedule, and the cross-chain authentication schemes.The experts claimed part of the chapter.

1. Future Meeting

• Next group meeting is scheduled for May 29th

1. Adjourn

• Motion # 3

Moved: Ping Lu Fuyun Network Technology Co. ,Ltd.

Seconded: ChunFeng Luo Hangzhou Yunphant Network Technology Co. ,Ltd.

Motion passed by voice vote without opposition

16：00 Adjourn