

深圳市地方标准  
征求意见汇总处理表

编号：

文件名称		金融行业区块链平台技术规范		文件种类	地方标准	
起草单位		深圳证券交易所、深圳前海微众银行股份有限公司、深圳证券通信有限公司、深圳市互联网金融协会、深圳市标准技术研究院、深圳前海联易融金融服务有限公司		立项日期	2018-05	
承办人		计胜侠	职务/职称	联系电话	0755-88668723	
序号	章条编号	意见内容		提出专家 (单位/联系方式)	处理意见	备注
1	封面	要么去掉英文译名有“一”，要么标准名称作空格处理，如“金融行业区块链平台 技术规范”；		深圳市标准 技术研究院 张旭杰 18682055312	采纳	
2	封面	英文译名各要素除第一个英文首字母大写，其他均应小写，需大写的专有名词除外。			采纳	
3	前言	增加涉及专利的声明，如“请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任”			不采纳	本标准不涉及专利
4	2 规范性引用文件	未发现正文引用该部分的标准，可放到参考文献位置，请核实。			采纳	
5	3	“下列术语和定义适用于本规范” 改为“下列术语和定义适用于本文件”			采纳	

6	3.1	注应另起一行		采纳	
7	3.6	联盟链术语定义中，一般而言之后的描述建议放在注里面		采纳	
8	6.2	增加“6.2.1 概述”章节标题（这里出现了悬置段）		采纳	
9	6.2	图 2 接入层应增加协议管理的功能模块		采纳	
10	6.2.1、 6.2.2、 .6.2.3 、 6.2.4、 6.2.5.1 ....	例如，增加“6.2.1.1 用户层功能”的标题，其他以此类推 认真检查其余出现的悬置段问题。		采纳	
11	未标明	“区块链技术”不如密钥算法及其它网络验证，如密钥函数构造选择协议算法等。另外，可考虑结合网络结算等金融基础平台。	名称单位不详，联系方式	不采纳	网络结算为应用服务，不属于区块链基础技术范畴
12	未标明	关于执业整体制度的改革建议	<1761929104@qq.com>	不采纳	本标准不涉及执业规范
13	6.2.3. 2.1	建议“防篡改”改为“不可篡改”	瑞霆律所 陆晖 18998996992	采纳	
14	3.1	定义修改		不采纳	一方面是定义引自成熟的其他标准，另一方面修改后将不能完整概况数据的相关事务

15	3.4	定义修改		不采纳	一方面是定义引自成熟的其他标准，另一方面，智能合约目前暂不具备法律合同效应
16	5.2	删除“可审计”		不采纳	本标准针对金融行业的区块链技术，需要支持“可审计”要求
17	6.2.3.3	建议区块链网络能追踪到用户		不采纳	区块链网络可以与传统互联网、以及金融机构的数据库系统进行结合，从而达到主体的追溯效果。区块链网络本身可以不涉及用户主体信息。
18	6.2.3.6.2	建议措辞修改：“不可抵赖性”		部分采纳	“不可抵赖性”改为“不可伪造性”
19	6.2.5.4.1	建议措辞修改：“可稽核”		不采纳	金融稽核亦称“金融内审”，是金融行业常见术语。
20	3 术语和定义	去中心化 Decentralization 去中心化是一种现象或结构，必须在拥有众多节点的系统或在拥有众多个体的群中才能出现或存在。节点与节点之间的影响。会通过网络而形成非线性因果关系。		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
21	3 术语和定义	节点 Node 由区块链网络的参与者操作的分类帐的副本。		不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
22	3 术语和定义	区块 Block 在比特币网络中，数据会以文件的形式被永久记录，我们称这些文件为区块。一个区块是一些或所有最新比特币交易的记录集，且未被其他先前的区块记录。	深圳比特时代技术服务 有限公司 黎耀钟 15768188269	不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
23	3 术语和定义	时间戳 Time Stamp 时间戳是指字符串或编码信息用于辨识记录下来的时间日期。国际标准为 ISO 8601。		不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
24	3 术语和定义	矿工 Miner 尝试创建区块并将其添加到区块链上的计算设备或者软件。在一个区块链网络中，当一个新的有效区块被创建时，系		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语

		统一般会给予区块创建者（矿工）一定数量的代币，作为奖励。		
25	3 术语和定义	矿池 Mineral pool 是一个全自动的挖矿平台，使得矿工们能够贡献各自的算力一起挖矿以创建区块，获得区块奖励，并根据算力贡献比例分配利润（即矿机接入矿池—提供算力—获得收益）。	不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
26	3 术语和定义	哈希值 Hash 一般翻译做“散列”，也有直接音译为“哈希”的。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。	不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
27	3 术语和定义	私钥 PrivateKey 私钥是一串数据，它是允许您访问特定钱包中的令牌。它们作为密码，除了地址的所有者之外，都被隐藏。	不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
28	3 术语和定义	公钥 PublicKey 是和私钥成对出现的，公钥可以算出币的地址，因此可以作为拥有这个币地址的凭证。	不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
29	3 术语和定义	主链 Main Chain 主链一词源于主网（相对于测试网），即正式上线的、独立的区块链网络。	不采纳	本标准更关注平台技术规范，无必要对所有基础的区块链术语进行定义。
30	3 术语和定义	侧链 Side Chain 楔入式侧链技术（pegged sidechains），它将实现比特币和其他数字资产在多个区块链间的转移，这就意味着用户们在使用他们已有资产的情况下，就可以访问新的加密货币系统。	不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
31	3 术语和定义	跨链技术 Cross chain Technology 跨链技术可以理解为连接各区块链的桥梁，其主要应用是实现各区块链之间的原子交易、资产转换、区块链内部信息互通，或解决 Oracle 的问题等。	部分采纳	增加 3.8 跨链技术 Cross chain Technology 实现不同区块链之间进行信息交互的技术。
32	3 术语和定义	硬分叉 Hard Bifurcations 区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。	不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语

33	3 术语和定义	软分叉 Soft Bifurcations 当新共识规则发布后，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
34	3 术语和定义	闪电网络 Lightning network 是指实现安全地进行链下交易，其本质上是使用了哈希时间锁定智能合约来安全地进行 0 确认交易的一种机制，通过设置巧妙的‘智能合约’，使得用户在闪电网络上进行未确认的交易也十分安全。		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
35	3 术语和定义	隔离见证 SegWit 把脚本签名数据从基本结构中剥离出来放到新的结构中，即原本一块处理的信息分开处理，例如在区块交易结构中交易信息和签名信息是一并处理的，现在把它拆分来处理，是一种分开验证、提升系统处理能力的技术。		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
36	3 术语和定义	零知识证明 Zero Knowledge Proof 证明者能够在不向验证者提供任何有用信息的情况下，让验证者相信证明者。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄露任何关于被证明消息的信息。		不采纳	本标准更关注平台技术规范，无必要对所有隐私算法的术语都进行定义。
37	3 术语和定义	区块扩容 Block expansion 区块扩容是指增加区块的容量。		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
38	4 缩略语	Dapp: 中心化应用 (Decentralized Application)		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
39	4 缩略语	DAO: 去中心化自治组织 (Data Access Object)		不采纳	金融行业区块链不涉及这类公有链和虚拟货币术语
40		无意见	深圳市华傲数据技术有限公司		
41		无意见	深圳市前海融资租赁金融交易中心有限公司		

