InSafe 安全区块链

技术白皮书

目录

1. 概述 3

2. 市场背景介绍 3

3. 平台目的 3

4. 平台架构 4

5. 运行机制 4

1) 联盟成员入驻机制 4

2) 成员信用机制 4

3) 仲裁机制 5

4) 高效查询接口机制 5

5) 行为追溯机制 5

6) 黑名单机制 5

7) 白名单机制 6

8) 威胁趋势机制 6

9) 信息共享机制 7

10) 数据防火墙机制 7

11) 智能定价机制 7

12) 用户众包机制 7

6. 技术框架 7

1) 海量数据处理 7

2) 高性能查询 8

3) 高效便捷接入 8

7. 价值 8

8. InSafe发展规划 8

9. 团队核心成员 8

# 概述

InSafe安全区块链（下称InSafe） 是一套基于区块链技术的自主研发的安全数据共享联盟链解决方案。InSafe着眼全球市场，通过区块链技术和安全业务模型的深度整合，在联盟成员间共享安全数据，将各个安全数据孤岛串联起来，形成真实可靠、覆盖面广的全球安全数据库，有效促进和完善互联网、物联网安全生态健康发展。 InSafe在用科技手段促进全球网络安全能力的提升上，具有划时代的意义。

# 市场背景介绍

只要是做IT相关的业务，都对应用环境安全、信息流转安全都有需求，受限于没有可靠的安全数据源，无法对应用环境进行检测。

* 安全数据采集开放通道少
* 安全数据中心存储，呈离散分布
* 跨机构使用数据，只能采取线下合作，使用代价高
* 物联网安全、互联网安全数据需求量大
* 随着5G网络、物联网、移动互联网的进一步发展，业务场景愈发多样化，将提出更多的安全需求

# 平台使命

利用区块链技术，链接全球信息安全数据，突破原有的安全行业数据壁垒，打造去中心化、可信、共享的安全数据产业联盟

# 平台组成

平台实行邀请制，构成角色分别为：

* InSafe基金会
  + 由InSafe创始团队组成，用于运营和维护InSafe区块链
* InSafe联盟成员
  + 由邀请入驻的全球各大互联网安全企业组成，是InSafe的主要成员，拥有数据使用权和仲裁权

# 运行机制

## 联盟成员入驻机制

为了保障平台数据的有效性和，InSafe平台建设初期，将采用邀请制，对入驻的企业进行严格的审查，设定联盟成员入驻门槛，入驻初期至少向链上提供500W条以上的有效数据。所有提供数据会在全链所有联盟节点进行审查，与链上数据重合率至少要低于50%。

## 成员信用机制

每个入驻的成员在初期都会分配给固定额度的信用积分，若发现成员违规行为，将会扣减信用积分，该积分只减不增。当积分扣为0时进行清退并永不可再次入驻。

## 仲裁机制

当联盟的某一成员对链上数据存在质疑时，可以发起仲裁，由所有联盟成员进行仲裁，将采用大于51%的投票作为最终结果。被仲裁过的数据如果要再次仲裁，需向InSafe基金会发起申请，由基金会发起二次仲裁。

基于数据属性和操作频度高的特点，所有仲裁均在线上自动化完成，每个入驻的联盟成员若要行使仲裁权利，需提供仲裁校验接口。

## 高效查询接口机制

InSafe提供全网查询接口，入驻联盟成员可以提供样本数据的MD5、SHA1、SHA256等信息进行数据属性的查询。联盟成员的查询次数取决于对链上数据的贡献，若贡献与查询的比值较低，则需要收取一定的ITC币作为补偿，并把补偿的ITC币按照一定比例分发给数据贡献高占比的联盟成员。非联盟成员可以通过支付一定量的ITC币换取查询次数。

## 行为追溯机制

为了更高效、安全的维护InSafe安全区块链上的数据，我们对链上数据做了重新定义，在链上记录了所有节点对数据的行为，包括数据的添加、定义、仲裁、冻结等操作行为。而数据本身则分离存放在联盟节点的本地数据库中，分离的数据受高强度的加密保护，且数据一致性与链上行为保持同步。联盟成员可以输入一个样本的唯一标识，可索引到样本当前属性、仲裁记录、数据添加记录等信息，可完整追溯一条样本的全生命周期。

## 黑名单机制

InSafe安全区块链保存着完整的黑名单数据信息，这些数据可以来自于各个平台（Windows、Linux、IOS、Android、MACOS），其信息包括但不限于：

* 是否为恶意样本/URL
* 样本类别（病毒、木马）
* URL类别

当入驻的联盟成员检测到某一恶意样本时，可以将该检测结果上报给联盟成员的InSafe节点，由该节点向全链进行广播校验，若此威胁信息已经存在于链上，则不记录该信息。若是首次发现此威胁信息，则记录在链上，并向全链广播。每上传一个有效的恶意威胁数据，都将给予该联盟成员奖励，形式包括但不限于发放ITC币等。若此威胁存在于链上但标记的信息并非威胁信息，则由该联盟成员对此样本发起仲裁。

## 白名单机制

InSafe安全区块链维护着全球最大的安全数据白名单，白名单链上数据可以由某个联盟成员主动添加，所有进入白名单的数据，都需要经过所有联盟节点的校验，全链联盟成员100%认可白名单属性，才可以进入InSafe区块链白名单。基于对白名单链中数据的保护，所有白名单数据仲裁仅可由InSafe基金会发起。

## 灰名单机制

问题1、灰名单是否要进入到InSafe主链中？

问题2、灰名单数据是否携带样本文件？

问题3、灰名单中的数据是否需要InSafe基金会使用VDC运营？

## 威胁趋势机制

InSafe接受所有联盟节点所上传的所有威胁信息，所有的威胁信息将被以不去重的方式对其发生频度进行记录，并在全链进行广播。每个参与的联盟成员节点可以通过查询接口得到目前全网动态实时的威胁发生趋势，更好的服务信息安全

## 信息共享机制

所有参与InSafe区块链的联盟成员，共享一份完整的、动态的链上安全数据。每个联盟成员均可以对链上数据进行查询、溯源。

在联盟成员的节点被创建的时候，会在链上分配一个全局唯一的身份ID，所有在链上进行的操作都需要携带这个身份ID，该身份ID会和一个ITC钱包地址绑定，所有ITC获取和消耗的结算都将发生在这个ITC钱包地址。

## 数据防护机制

为了防止安全区块链上的数据被恶意爬取和破坏，InSafe设立数据防火墙，实时检测数据状态，当发现异常时立刻发出警告，并扣减该节点相应的信用积分，情节严重将直接清退。

## 智能定价机制

为了InSafe生态的良性运转，对链上的数据进行查询所消耗的ITC量会根据数据量级、查询指数等指标对ITC进行动态智能“定价”，避免ITC市场定价发生浮动时联盟成员使用数据受阻

## 用户众包机制

InSafe基金会鼓励所有联盟成员利用ITC市场进行用户众包行为。

项目初期，InSafe基金会将发起“全民安全计划”，利用基金会现有资源，将恶意数据发现、样本分类标注、样本采集上传等任务在全球范围进行分发，并根据收集结果的准确程度和量级，奖励给用户ITC币。同时所有收集来的安全数据都将通过InSafe基金会进入到安全区块链中。

# 技术框架

## 海量数据处理

相比于常规区块链，安全区块链要支撑对海量数据的分析和处理，InSafe对链交易验证算法做了优化，将链前向检查由对单个区块的检查改为对区间链的检查，对相连的区间链进行前向索引，直到第一个区块被校验，以此来确保海量数据交换的可信度，同时极大的降低了数据入链时，链前向检查的耗时。

InSafe对PBFT共识算法进行优化，极大提高了区块数据的写入效率。同时对网络通信进行了优化，提高联盟节点间数据广播、数据同步的速度，确保链上数据的及时性。

## 高性能查询

InSafe区块链将操作数据行为和数据本身做分离，在区块链中记录的是某一成员实体对某一条数据进行的某一项操作的行为，而对应的安全数据被分布存储在数据库中，可以根据不同的业务场景提供高效快速的查询服务。

## 高效便捷接入

联盟入驻InSafe区块链只需提供一台可以接入互联网的服务器即可，操作系统可同时支持Windows和Linux。InSafe提供全套的SDK支持，帮助成员0开发成本接入。

# 价值

对我们：

* 拥有全球安全大数据；
* 可孵化收费安全项目；
* 非安全类公司加入联盟费用；
* ITC币收益。

对联盟：

* 安全数据；
* 非安全类公司加入联盟费用按权重分成；

对用户：

* 联盟所有用户安全能力提升；
* 用户可能产生ITC币收益。

# InSafe发展规划

安全数据区块链 -> 大数据区块基础链 –> 孵化其他数据区块链应用

# 团队核心成员