

卫士链——基于区块链的数字资产保险平台

郭玉荣, 冼祥斌, 杨振国, 刘文印

广东工业大学计算机学院, 广东 广州

Email: 867837489@qq.com

收稿日期: 2021年3月21日; 录用日期: 2021年4月15日; 发布日期: 2021年4月22日

摘要

区块链(Blockchain)是一种分布式可共享的、通过共识机制可信的公开账本。纵观区块链发展的历程, 区块链已经从最早的“为币而生”逐渐发展成为贯穿信用、银行、保险、安全等各行各业的“革命者”。卫士链是一个基于国内最大公链纳世链技术的开放式的数字资产的保险平台, 卫士链项目借鉴了伦敦劳埃德保险社的理念, 一个交易数字资产保险的风险市场, 是一个去中心化的“劳合社”, 为希望转移风险的人与愿意承接风险的企业和个人提供交易平台。本文主要设计了基于区块链的网络身份安全数字资产保险系统平台, 在卫士链平台上参与者都可以是保险发行人, 保险发行人可以根据用户的个性化需求使用智能合约提供个性化的定制保险服务, 构建针对两种用户群的提供保险服务模型, 包括个人网络身份安全数字资产保险和企业数据库安全保险, 在评估索赔阶段自动触发智能合约自动理赔, 构建一个稳定的区块链保险平台, 其保费由动态定价模型来决定, 解决了传统保险公司对于网络数字资产不敢保, 理赔条款不到位, 保险保费不透明的问题。

关键词

区块链, 数字资产, 智能合约, 动态定价模型

WisChain-Blockchain—Based on Digital Asset Insurance Platform

Yurong Guo, Xiangbin Xian, Zhenguo Yang, Wenyin Liu

School of Computer Science and Technology, Guangdong University of Technology, Guangzhou Guangdong

Email: 867837489@qq.com

Received: Mar. 21st, 2021; accepted: Apr. 15th, 2021; published: Apr. 22nd, 2021

文章引用: 郭玉荣, 冼祥斌, 杨振国, 刘文印. 卫士链——基于区块链的数字资产保险平台[J]. 计算机科学与应用, 2021, 11(4): 938-947. DOI: 10.12677/csa.2021.114097

Abstract

Blockchain is a distributed, shareable, and trusted public ledger through a consensus mechanism. Throughout the development of the blockchain, the blockchain has gradually developed from the earliest “born for currency” to a “revolutionary” that runs through various industries such as credit, banking, insurance, and security. Our WisChain is an open digital asset insurance platform based on the technology of the largest public chain in China. The WisChain project draws on the concept of London Lloyd Insurance Company, a risk market for trading digital asset insurance. A decentralized “Lloyd’s” provides a trading platform for people who want to transfer risks and companies and individuals who are willing to take risks. This article mainly designs a blockchain-based network identity security digital asset insurance system platform. On the Wischain platform, all participants can be insurance issuers, and insurance issuers can use smart contracts to provide personalized customization according to the individual needs of users. Insurance services, build insurance service models for two user groups, including personal network identity security, digital asset insurance and corporate database security insurance, and automatically trigger smart contracts to automatically settle claims during the evaluation of claims stage, building a stable blockchain insurance platform. The premium is determined by a dynamic pricing model, which solves the problem that traditional insurance companies dare not protect digital assets on the Internet, the claim clauses are not in place, and the insurance premiums are not transparent.

Keywords

Blockchain, Digital Assets, Smart contract, Dynamic Pricing Model

Copyright © 2021 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

大多数人每天浏览着各种各样的网站和使用各种各样的软件，因此现实中的人在网络虚拟空间上也拥有许多网络身份数字资产(这里的网络身份主要指的是人们在不同网站或软件上所注册的登录用的账号和密码)。网络不仅承载着大量的一般资源信息，也容纳了许多重要的私人信息，所以网络带给人们便利的同时，也潜藏着私人信息泄露的风险[1]，尤其是个人账号密码的泄露会带来实际利益的损失。黑客攻击防不胜防，因为大多数网站仍然存在许多未知漏洞，一旦被黑客攻破，则会导致不可估量的损失。现实中的利益损失人们可以通过购买保险来获得补偿[2]，但目前很少有保险公司会赔偿信息资产的损失，因为这种损失难以估量而且证据不足，甚至网站可以伪造证据骗保，并且使用区块链技术可以让用户在购买保险时采用匿名的形式，防止个人重要身份信息泄露。并且区块链技术中的分布式账本和不可篡改的性质可以解决信息的不对等和伪造，建立在区块链技术的网络身份安全保险不仅能让保险公司放心地提供保险业务，还能提升已购买保险的网站的市场竞争力。当然，针对个人用户的保险也可以降低个人账号密码泄露后的损失。近几年网络安全威胁如图1所示。

区块链技术在近几年爆炸式的发展大家有目共睹，区块链的技术特点“去中心化”、“开放性”、“防篡改性”、“匿名性”、“可追溯性”都完美的符合保险行业。并且保险公司的盈利能力取决于索赔支出的数量和所收取保费的数量，尽管目前有监管部门对保险的公司进行严格的监管监督，但是传统

的保险公司也存在着理赔条款不透明, 理赔不到位的情况。此外还由于保险公司对于大数据的风险评估的依赖及其决策保守的性质, 对于其新型的数字资产的保险产品的缺口无法填补。

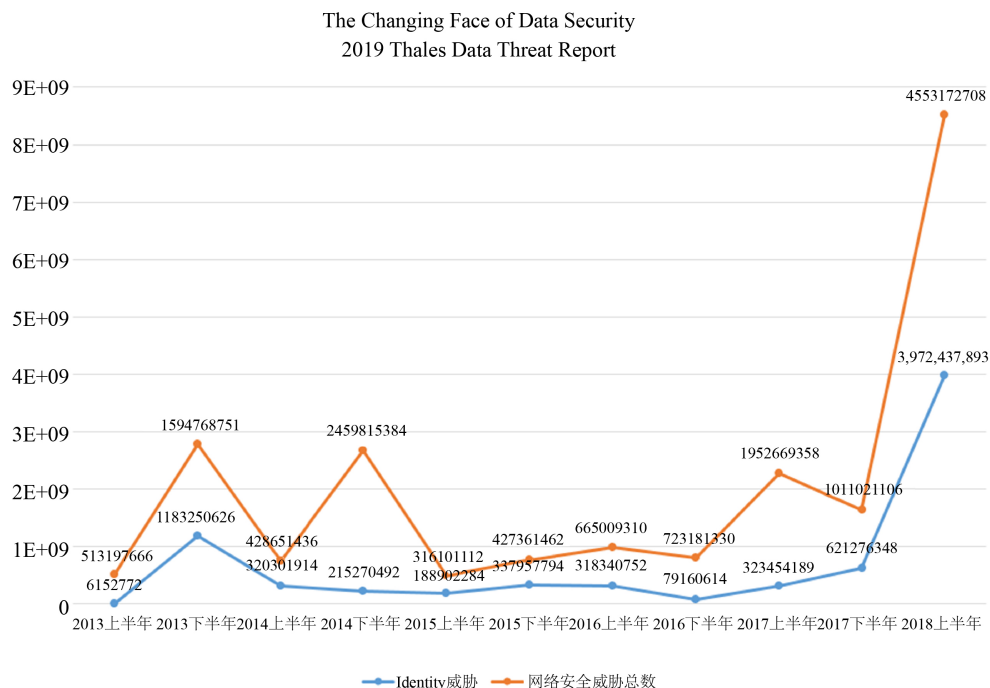


Figure 1. Network threat line chart
图 1. 网络安全威胁折线图

互联网的飞速发展已经使得个人的数字资产的价值, 以及企业数据库资源和员工的个人资料信息的价值大大增加, 但是传统的保险行业明显对于数字资产这一部分的保险产品的供给不足。卫士链基于国内最大公链纳世链[3]提供的开放式的数字资产平台很好的解决了数字资产保险产品的缺失问题, 卫士链允许任何人成为数字资产的保险发行人, 也允许任何人成为被保人, 与常规保险行业不同的是, 常规保险是由发行人取决于对于保险理赔的判断, 但卫士链是通过采用智能合约[4]预言机的形式摆脱了这些不平等的判决。

由于传统的保险公司难以提供让个人用户和企业网站满意的新型网络身份数字资产保险产品, 本文设计了一种基于区块链的数字资产保险平台, 其中包含: 匿名投保、智能合约个性化定制保险、动态定价模型等关键技术。

2. 区块链保险相关研究

对网络服务提供保险最早由 Liu Wenyin 等提出, Liu Wenyin 等指出对网络服务提供保险的重要性及可行的商业模式[4]。网络服务涵盖了整个互联网。近年来, 保险业在网络世界也逐渐获得发展。

对网络服务的保险主要有两个方面, 一个是对网站提供保险, 一个是对具体软件(需要连接互联网)提供保险。前者如 360 安全公司, 当用户加入 360 安全协议之后, 通过点击 360 搜索推广网站, 因该推广网站属于钓鱼、诈骗网站或假冒他人官网或授权网站, 导致用户发生直接财产损失, 可以申请先行赔付。当用户符合赔付条件, 配合 360 进行调查取证, 且证据充分的, 360 工作人员审核无误后可按照《360 搜索推广赔付协议》赔付款项。用户应当在财产损失发生之日起 30 日内(包含 30 日)向 360 提出赔付申请,

超过该有效区间, 则用户不能通过本计划获得赔付[5]。

后者则是软件的开发商提供一个保险平台, 如 Alibaba 公司的支付宝 APP 提供的保险平台使得传统的保险公司把传统的保险项目利用网络的形式线上进行推广[6], 让用户购买, 虽然说是网络保险, 但实际内容却和传统的保险内容是一致的。不管哪种方式, 都需要对购买保险者绝对的信任, 并且都需要在客户端实名认证, 这就加大了个人隐私泄露的风险[7]。而且网络流量数据仅保存在购买保险者一端, 购买保险者可以伪造证据骗保, 保险协议当中也会存在跟传统保险相同的问题, 例如: 隐藏条款、信息不对称等。

在 2017 年底, 法国安盛 AXA 航空公司推出航空保险产品 Fizzy [8], 该产品在以太坊区块链上的智能合约里面存储了保险内容条款。当用户乘坐的航班延误时, 会触发以太坊当中的智能合约保险条款, 该合约与全球空中交通数据库网络相连。如果航班延误超过 2 小时, 那么该航班的保单持有人将触发智能合约自动获得赔偿。AXA 代表 Jean-Baptiste Mounier 说过智能合约决定我们是否应该赔偿投保人, 并触发我们的赔付系统。使用智能合约来自动触发索赔, 可以很好的增加保险公司和被保险人之间的信任关系, 中间不会存在保险公司抵赖不赔付问题, 也不存在被保险人保单造假的问题。虽然基于区块链技术的航空险可以使用智能合约进行自动理赔, 但是跟本文研究的基于区块链的数字资产保险有实质性的区别。

根据上述的国内外的研究发现很少有平台和保险公司为网站的数据库和个人身份安全提供保险, 因为缺少专业的安全知识对网站和软件做安全评估继而提供保险, 更无法检察出骗保行为。

3. 卫士链的工作原理

从图 2 中就可以看出, 除了区块链作为卫士链系统平台的数据库外, 卫士链还涉及五个重要的部分, 即卫士链社区、专业团队(保险公司或者是专业的保险经纪人)、积分池、积分盈余池、保险理赔积分。区块链主要存储交易用户的哈希数据, 专业团队、和卫士链社区的参与者负责把交易数据打包上链, 并且专业团队会评估每个链上交易保险的合理性, 所有的交易积分会按照一定的比例存放在积分池、积分盈余池、保险理赔积分。

卫士链的系统架构图, 如图 2 所示。

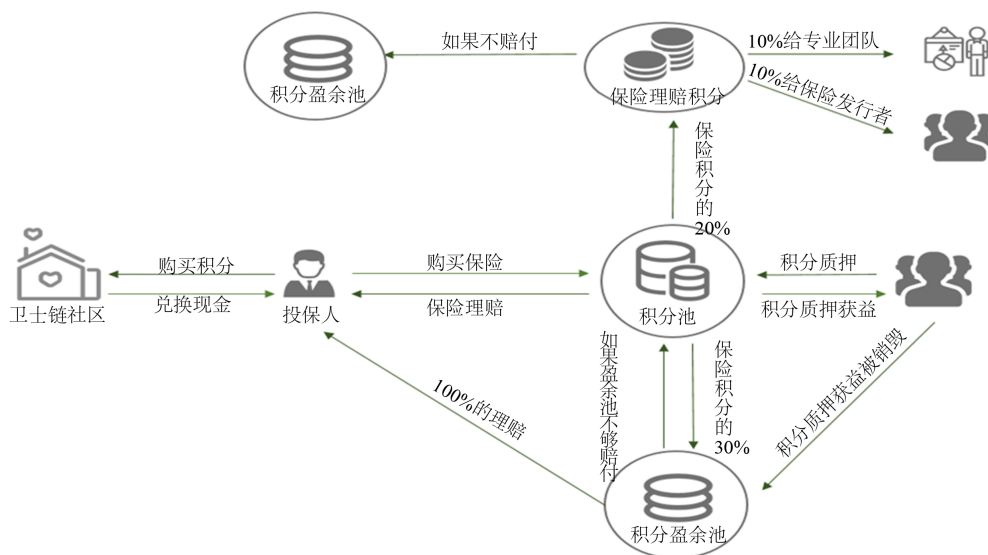


Figure 2. WisChain system architecture
图 2. 卫士链系统架构

3.1. 积分池

积分池制度是支持卫士链平台业务发展的重要模块，卫士链的积分将奖励给卫士链的保险发行人和被保险人，每生产一个区块，20个积分将按照比例分配给所有提供贡献的参与者。

奖励所获取的积分可用于 1) 承担保险风险并赚取保费。2) 持有积分并且享受卫士链的社区价值增长所带来的受益和社区提供一些积分杠杆服务。3) 可以在社区内部转让或者销售积分实现价值。

在积分奖励的支持下，保险业务将为积分持有人带来可观的利润，这一系列的社区生态会使卫士链积分的价值增长，较高的积分价值可以吸引更多的积分持有人维护卫士链保险社区生态[9]，保证卫士链社区向积极的方向发展。

当积分盈余池的积分不满足于最低的积分要求是，积分盈余池的奖励交易将被冻结，直到积分盈余池的积分池满足最低需求的时候，积分奖励才会继续进行，这是由于有新的积分进入积分盈余池或者是由于积分制度的改变。

当积分盈余池不能满足所有的保险理赔时，将会使用积分池的积分支付剩余的所欠积分，积分模型用于监控卫士链保险平台的风险，并给积分池提供有吸引力的风险调整后的积分收益，积分持有人可以通过判断积分盈余池的积分状况，判断卫士链社区的运营状态。为了吸引更多的人参与卫士链平台提供的保险业务，平台上的积分持有人通过积分制度努力给卫士链社区做贡献。

对于保险产品来说，保险定价就是依据过去事故发生评估风险可能性，并且这种风险的发生的可能性是可观可衡量的，这也是一个保险产品确定保费的重要依据。大数定律是，当足够多的相同性质的事件发生时，它们的风险概率将越来越接近实际概率，从而可以获得更准确的估计。由于现实生活中每个人的思维方式有所不同，因此不能认为它是独立且分布均匀的，所以在卫士链的动态定价模型里使用切比雪夫大数定律更为合理。

假设 $x_1, x_2, x_3, \dots, x_n$ 是一组独立的随机个体的，其中的每一个具有的预期值 $E(X_k)$ 和方差 $D(X_k)$ 。如果存在一个使 $D(x_k) \leq c$ ($k = 1, 2, \dots, n$) 的常数 MCR，则对于任意正数 ε ，公式

$\lim_{n \rightarrow \infty} \left\{ \left| \frac{1}{n} \sum_{k=1}^n x_k - \frac{1}{n} \sum_{k=1}^n E x_k \right| < \varepsilon \right\} = 1$ ，随着人数的增加，即 $n \rightarrow \infty$ ，获得的均值将越来越接近实际均值。

由于当前缺乏有关智能合约发生漏洞可能性的历史数据，所以刚开始合约定价成本会很高，但是随着之卫士链智能合约被调取次数的增多，调取智能合约成本会逐渐降低。卫士链不用使用单个集中实体来设置溢价率，也不用由保单发行人与被保险人之前进行保费金额的谈判，而是根据动态定价模型所提供的价格进行投保。我们假设风险遵循 beta 分布[10]，其公式(1)如下：

$$X \sim \text{Beta}(\alpha, \beta) \quad (1)$$

其中 α 是出售的保单所提供的总金额， β 是为此类风险提供支持的总金额，然后计算出最终保费，其公式(2)如下：

$$P\{X \leq \text{风险花费}\} \geq 95\% \quad (2)$$

额外的 20% 将加载到“风险成本”中，以获取最终的保单价格。

3.2. 购买保险

社区新用户在第一次在卫士链平台购买保险时，用户账户没有购买保险所需要的积分，这时用户需要去卫士链社区使用现金兑换积分，从而使用积分购买保险。

当个人用户和企业用户购买数字资产保险时，用户提出自己的需求，被保内容，被保内容的价值和

被保日期时，卫士链会生成一份保险需求，这份需求会通过区块链广播给保险发行人，保险发行人会根据用户需求，使用智能合约的形式生成一份智能合约，这份智能合约会传回给用户，用户看到智能合约之后，再确定是否对数字资产进行投保。不管用户采用或者拒绝，保险发行人都会得到积分奖励，若用户采用此智能合约，保险发行人的积分奖励由用户的保费承担，但若用户拒绝使用此份智能合约，保险发行人的积分奖励将由积分盈余池支付。用户不可恶意拒绝智能合约，必须给出合理理由，由积分持有者进行投票，积分持有者的投票资格由积分质押获得，无积分质押者不符合投票条件。当超过百分之七十的投票者认为拒绝合理，用户可以拿到奖励积分，若是拒绝不合理，会对用户进行投保积分百分之三十的扣除，扣除的积分用来奖励投票者和保险发行人。

投保人除了参与保险，还可以获得卫士链积分质押[11]，将自己现有积分进行质押，获取更多的积分，积分质押的项目可以由投保人自由选择，一个保单，对应两次积分质押项目的次数。这一机制会给卫士链吸引更多的参与者。参与者越多每个用户的数字资产的保险需求也不一样，这样也会促使卫士链数字资产保险更多元化。

当投保人投保的保单在保险期内，满足合同条约的赔付时，卫士链将自动启动赔偿的请求，卫士链的去中心化自治组织将启动一个或者多个投票，投票通过则根据合同条款进行自动赔偿，不通过会给出拒绝理由，投保人根据拒绝理由可以再次申诉，申诉次数不可超过三次，避免造成资源浪费。

在投保过程中一定会有个人隐私身份信息的传递，这样会增加个人隐私泄露的风险，为了减少这一风险，将使用重加密技术加密隐私数据[12]，让除了保险公司之外的人无法拿到隐私数据，其他人想要获得用户隐私数据，必须得到用户授权，让用户自己控制权限。

具体步骤如下：

- 1) A 用自己的公钥加密明文 M ， $C_A = E_A(M)$ ， M 是 A 想要给 B 的东西， E 是非对称加密算法，例如经典 RSA。
- 2) B 将请求发送给 A，然后由 A(或代理)生成一个转换密钥 $PK_{A \leftrightarrow B}$ 。
- 3) A 将 C_A 和 $PK_{A \leftrightarrow B}$ 发送到卫士链社区。
- 4) 该卫士链社区使用 $PK_{A \leftrightarrow B}$ 将密文 C_A 转换为 C_B 。在此， C_B 是用 B 的公钥加密的 M 的密文。在该步骤中，卫士链社区仅提供转换服务，而不能获得明文。
- 5) 代理将密文 C_B 发送给 B。
- 6) B 用自己的私钥解密 C_B 以获得明文 M 。

3.3. 积分盈余池

每当投保人支付保费时，积分盈余池就会累计起来，将支付保费的 30% 的积分增加到积分盈余池中，另外的 20% 的积分将保留到保险合同期满，如果此单保险没有发生索赔，这 20% 也将放置到积分盈余池中。随着时间和参与者的增多，积分盈余池的积分不断增长，首先盈余池的积分将用来支付保险索赔，当盈余池中的积分无法满足所有的保险索赔的时候，就会启动积分池的积分索赔。当积分盈余池的积分足够多的时候，积分质押项目的受益就会不断减少，积分价值就会降低，为了卫士链社区平稳运营，社区参与者可以进行投票，将积分盈余池的积分进行部分销毁，以维持社区积分价值。

3.4. 积分质押

投保人和保险发行人可以将自己剩余的积分质押在不同的项目上面，获取溢价积分，一个项目最多可以获取 50% 的保费，但是这个数字不是固定的，一个保险项目质押的积分越多，那么质押所获的积分越少，当一个保险项目，质押的积分少与保费的 10% 的时候，质押积分的受益翻倍，相应的这个保险的

保费更贵，保险项目质押的积分越多时，这个保险越便宜，质押受益越低。

如果索赔成功，积分盈余池会赔付保险积分金额的 50%，剩余的 50% 由质押积分者赔付，一旦触发索赔合约，积分质押的积分会全部锁定，直至赔付完成，剩余的积分会退回到参与者账户。

4. 共识机制

卫士链平台主链使用的是 POC (Proof-of-Capacity 容量证明) 共识机制，相比于传统的 POW (Proof-of-Work 工作量证明) [13]，POC 的优势极为明显，POC (容量证明机制) 简单来说就是利用计算机硬盘中的闲置空间进行存储来进行质押挖矿获取收益，通过某种既定的算法产生数量众多的伪随机数，并将这些随机数存入硬盘，在竞争打包区块的时候，只需要通过扫盘(也可以称作读盘)——随机加以匹配来打包区块。

这样区块的生成是由存储设备的存储密度大小决定，从物理上限制了区块的生成，保障区块链的安全，最终使整个区块链达成共识。

卫士链的模块化架构设计支持在共识机制中插入新的功能模块以及发生黑客攻击防止功能模块宕机也可以立刻替换核心功能模块，社区参与者可以共同投票为社区设定自己的规则，并根据社区的需要进行自定义。

4.1. 信用等级

信用等级是用来约束卫士链平台用户恶意破坏平台稳定，利用系统漏洞进行非法牟利的系统，信用评级系数介于-1 到 1 之间，用户初次加入卫士链时，用户的信用评级都是 0，用户可以参与卫士链的保险项目，或者平台的各种投票活动，项目质押，社区维护建议等，卫士链将会根据信用评级的算法，合理的增加或者减少用户的信用评级系数，当平台参与者的信用系数低于-1 时，就会被卫士链检测，当作恶意节点剔除掉，此地址将无法参与卫士链的任何保险项目。当用户的信用评级系数达到 1 时，用户在卫士链项目的积分收益会增加 20%，信用评级系数达到 1 的用户不是无限增加的，评级系数为 1 的用户只占参与者的百分之 1，信用评级系数为 1 的用户行为也会一直接受卫士链的检测，信用评级系数越接近 1 的用户，有做恶行为，卫士链的降级系数惩罚会更加严格。同理当部分信用等级系数在-0.95~-1 之间的用户[14]，要是继续作恶破坏社区运营，惩罚也会更加严格，若是为卫士链做出贡献参与项目，投票活动等，这些信用等级较低的用户信用等级会增长得比较快，当分数越靠近 0，信用等级的增长则会恢复到正常水平。

4.2. 通报警告

当参与节点因为网络原因或者是计算机崩溃问题时未能及时生成块，这种不会被卫士链认为是恶意破坏链的行为，但是由于这会影响到整个卫士链系统，所以由于网络问题或者设备崩溃会全网广播警告，要是第二次又出现同样的问题，就会降低信用等级。

假设在某一时间节点，ABCD 四人拥有一致的账本，这时 B 告诉 C 有个节点交易失败，这笔交易会由 B 广播给网络中的其他人。但 ACD 收到 B 的广播之后不会马上记入自己的账本上，因为还需要验证交易的合理性，验证之后，才会更新到各自的账本上。

4.3. 移除节点

若卫士链发现恶意攻击、双花攻击或者试图分叉系统故意尝试攻击其他节点的情况下，卫士链能够检测并且启动修复程序，避免造成损失。并且在第一时间会冻结恶意节点的积分，冻结时间长达 60 天，并且将其节点的信用等级设置为-1，这就意味这个节点不能参与系统的任何项目，直接移除节点全网广

播，如算法 1。

Algorithm 1. Removing authorities

算法 1. 节点退出

Algorithm 3 Participation to the consensus when removing nodes

Removing leader node:

```

function RemovingLeader(c)
  Inform the blockchain network that a txs should be sent to new config;
  if self in the nodes to remove then
    stop confirm transactions
    start transmitting the queued txs to the new config
    when the node has no transaction left do
      shut down
    end
  else
    perform consensus with new configuration
  end if
end function

```

4.4. 保险理赔

当用户发起保单理赔之后，提交理赔证据，触发了理赔的智能合约，流程如下图 3 所示。

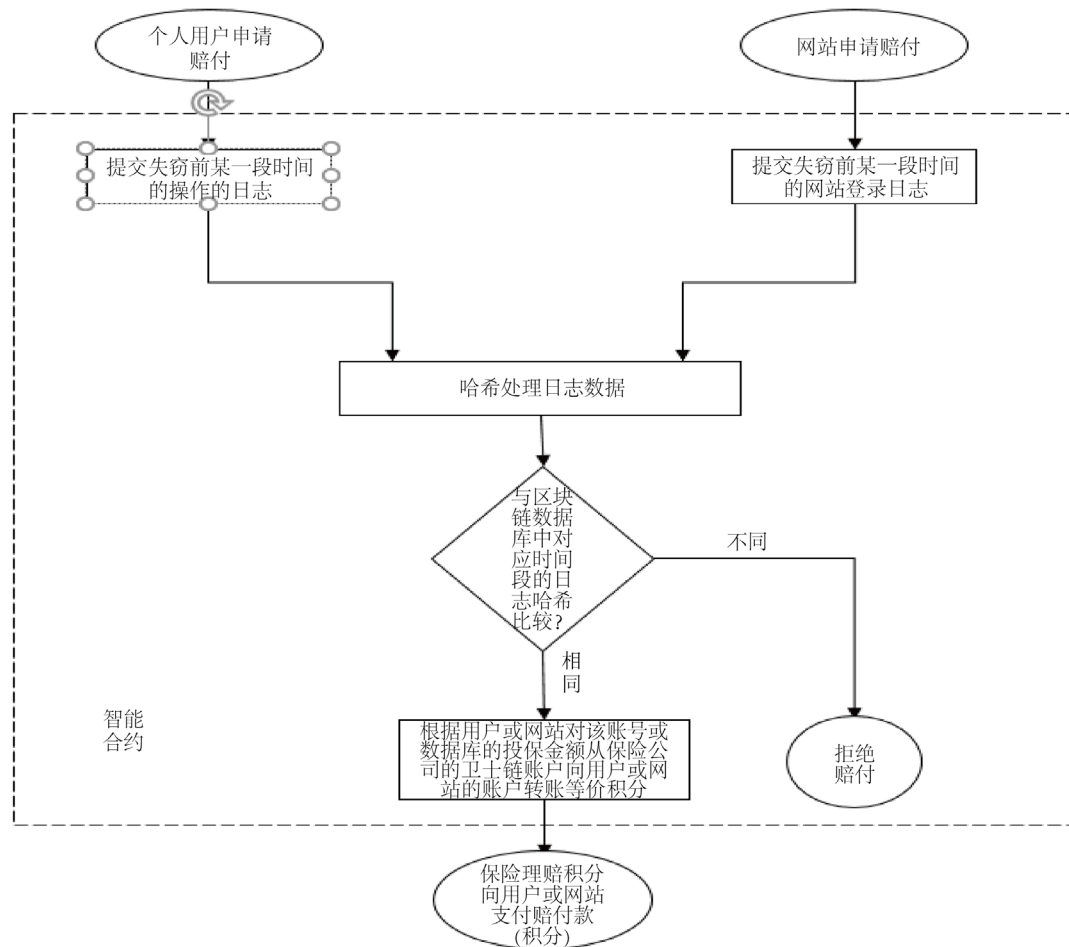


Figure 3. Insurance claims

图 3. 保险理赔流程

5. 实验与分析

为了验证本文卫士链平台系统的效率，基于 Java 语言在 NULS 公链上面搭建了私有环境，采用多机器多节点模拟共识进行，本次实验在 1 台 Intel i7-7700 CPU、16 G 内存、512 硬盘、操作系统为 CentOS 7.6 64 位的云服务器上进行。

和现有市场上的保险以及区块链保险产品进行比较，卫士链有以下优化(图 4)。

	产品特征
360 网购先赔	必须使用手机端的 360 浏览器和 360 安全卫士
支付宝帐号险	把线下的保险搬到线上销售，理赔需人工查验
InsurChain—区块链基础上的保险生态	建立一套新的保险生态，减少中间环节，降低成本
卫士链	设计新型的数字资产保险，降低保费，理赔自动化，形成一个良性循环的社区

Figure 4. WisChain comparison of advantages

图 4. 卫士链优点对比图

根据实验分析来看，市场上只有和区块链相关的保险，并没有类似的基于区块链的数字资产保险，卫士链提出的数字资产保险是非常具有创新性的。

6. 总结与展望

针对传统保险的痛点问题，卫士链可以通过智能合约完成所有的保险内容、投保、理赔等所有操作，但是实际上，为了考虑到所有参与者的利益，更好的实现去中心化，并保证所有投保和理赔过程的透明化，某些时间的解决还需要依赖社区参与者的投票，因此，卫士链平台还会建立一个去中心化自治组织，以解决此类决策问题，但是这个去中心化的自治组织没有任何权利管理积分池，也不能将积分分给任何人，除了参与决策没有其他任何权利，每个去中心化自治组织的成员可以随时通过投票由其他参与者代替。

基金项目

广东省基础与应用基础研究基金(No.2020A1515010616); 广东省引进创新科研团队计划资助项目(2014ZT05G157)。

参考文献

- [1] <https://legaltranz.com/archives/120265>
- [2] <https://baike.baidu.com/item/%E5%8A%B3%E5%90%88%E7%A4%BE/3975030?fr=aladdin>
- [3] <https://www.nuls.io/partnerships/>
- [4] Liu, W., et al. (2011) Business Models for Insurance of Business Web Services. In: IRMA, ed., *Global Business: Concepts, Methodologies, Tools and Applications*, IGI Global, Pennsylvania, 261-272.
- [5] Frauenthaler, P., Sigwart, M., Spanring, C., Sober, M. and Schulte, S. (2020) ETH Relay: A Cost-efficient Relay for Ethereum-Based Blockchains. 2020 *IEEE International Conference on Blockchain*, Rhodes, 2-6 November 2020 204-213. <https://doi.org/10.1109/Blockchain50366.2020.00032>
- [6] Moschou, K., et al. (2020) Performance Evaluation of Different Hyperledger Sawtooth Transaction Processors for Blockchain Log Storage with Varying Workloads. 2020 *IEEE International Conference on Blockchain*, Rhodes, 2-6

-
- November 2020, 476-481. <https://doi.org/10.1109/Blockchain50366.2020.00069>
- [7] Kuperberg, M. (2020) Towards Enabling Deletion in Append-Only Blockchains to Support Data Growth Management and GDPR Compliance. 2020 *IEEE International Conference on Blockchain*, Rhodes, 2-6 November 2020, 393-400. <https://doi.org/10.1109/Blockchain50366.2020.00057>
- [8] Singla, V., Malav, I.K., Kaur, J. and Kalra, S. (2019) Develop Leave Application Using Blockchain Smart Contract. 2019 *11th International Conference on Communication Systems & Networks (COMSNETS)*, Bengaluru, 7-11 January 2019, 547-549. <https://doi.org/10.1109/COMSNETS.2019.8711422>
- [9] Nguyen, T.Q., Das, A.K. and Tran, L.T. (2019) NEO Smart Contract for Drought-Based Insurance. 2019 *IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, Edmonton, 5-8 May 2019, 1-4. <https://doi.org/10.1109/CCECE.2019.8861573>
- [10] Shaw, S., Grant, D.B. and Mangan, J. (2021) A Supply Chain Practice-Based View of Enablers, Inhibitors and Benefits for Environmental Supply Chain Performance Measurement. *Production Planning & Control*, **32**, 382-396. <https://doi.org/10.1080/09537287.2020.1737977>
- [11] Abubashim, A. and Tan, C.C. (2020) Smart Contract Designs on Blockchain Applications. 2020 *IEEE Symposium on Computers and Communications (ISCC)*, Rennes, 7-10 July 2020, 1-4. <https://doi.org/10.1109/ISCC50000.2020.9219622>
- [12] Yu, Y.N. and He, Y. (2021) Information Disclosure Decisions in an Organic Food Supply Chain under Competition. *Journal of Cleaner Production*, **292**, Article ID: 125976. <https://doi.org/10.1016/j.jclepro.2021.125976>
- [13] Agrawal, T.K., Kumar, V., Pal, R., Wang, L. and Chen, Y. (2021) Blockchain-Based Framework for Supply Chain Traceability: A Case Example of Textile and Clothing Industry. *Computers & Industrial Engineering*, **154**, Article ID: 107130. <https://doi.org/10.1016/j.cie.2021.107130>
- [14] Di Nora, C., Sponga, S., Ferrara, V., *et al.* (2021) Emerging Therapy in Light-Chain and Acquired Transthyretin-Related Amyloidosis: An Italian Single-Centre Experience in Heart Transplantation. *Journal of Cardiovascular Medicine*, **22**, 261-267. <https://doi.org/10.2459/JCM.0000000000001094>