

WISCHAIN

全球唯一网络身份安全卫士链

<https://wischain.denglu1.cn>

1 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”。经过在区块链行业的深耕积累, 我们清晰的看到, 未来区块链的价值绝不仅限于数字货币。赋予区块链在商业中的价值, 使其为传统的商业模式注入新鲜的活力, 这才是我们打造区块链产品的使命。本文在一款名为登录易 (DengLu1.cn) 的网络身份安全产品的基础上提出了一种基于区块链的网络身份安全保险系统, 名为卫士链 WISChain, 为最终用户的个人网络身份安全和商业网站的数据安全提供了两种保险服务模型。索赔证据 (包括使用登录易的日志) 会自动上传到区块链以保证其真实性。保单以智能合约的形式上链, 出险时自动执行, 可以在保险公司和保单持有人之间建立信任。WISChain 为支持商用网站和个人用户的对帐号、密码和网站安全提供了基于保险的保障。本文将详细说明 WISChain 架构、技术特色与优势和应用案例。

2 前言

区块链的商业价值, 已经通过比特币, 以太坊等区块链项目得到了最好的印证。数字加密货币通过去中心化发行, 链上数据不可篡改等特性为广大用户所接受。当前, 很多数字加密货币区块链项目都形成了相对稳定的生态。然而, 由于

区块链自身与外界封闭的特性，目前这些区块链生态形成了一个彼此隔绝的孤岛。除了，BTCRelay 等少数项目在链间的交互上做出了探索之外，最常见的还是独立于链外的数字货币交易所这样的机构，通过传统的运营模式将区块链当做金矿，把数字货币当作货物来交易，这种方式只能发挥出区块链有限的价值。

纵观互联网的发展历程，以及发生的巨大变革，我们无法否认通信所具有的巨大力量。其实区块链的诞生本身就是带着互联网的前瞻性的，在不依赖中心化服务的的情况下，节点之间通过 P2P 协议通信，共识，备份数据，创立了彼此之间的信任。互联网发展至今，越来越深刻地体会到骨干网络负荷增加，攻击频发等弊病所带来的隐私泄漏，财产损失，名誉损失等一系列的问题，并积极寻求解决方案。例如，企业购买了我们的 WISchain 产品之后，我们会和专门的安全公司合作对网站进行漏洞评估，安全评级等安全措施，提高企业网站安全性，减少被黑客攻破的成功率，并且在企业网站受到攻击之后，根据企业的受损情况对投保企业进行理赔。对于个人保险用户来说，相对比较简单，只需要在登录易内部购买账户身份安全保险，使用登录易登录的所有网站的账户，密码都可以投保。要是使用登录易登录发生帐号密码等泄漏的情况，用户提供泄露凭证即可即时理赔到账。

2.1 区块链行业瓶颈

比特币的诞生开启了区块链 1.0 时代。比特币由于其产量恒定、产量递减等特性，具有价值储藏功能，被视为数字黄金得到投资者的追捧。但也由于性能低下以及资源的大量消耗，广泛受到诟病。

基于以太坊的区块链 2.0 时代的到来,虽然由于其设计的智能合约使不同数字加密货币之间的交换变得更加容易,不再仅仅局限于比特币一种数字加密货币的交换,被证明是一个高效的通证众筹平台。基于以太坊的高效通证众筹平台,为区块链技术及行业发展与资本投资的对接提供了通道,为全球化参与区块链行业发展与共建提供了基础。然而脱离通证发行的层面,以太坊仍然没有提供一个能够用于大众日常生活中的价值交换平台。为了找到真正具有商业价值的区块链解决方案,全球范围内的区块链公司仍然在不断探索。

在基于区块链的未来新世界中,人们需要一个能够真正触及日常生活方方面面,支持众多的保险消费场景,为普通人和企业提供价值的区块链生态。而目前区块链技术和数字加密货币的发展仍然存在较多的瓶颈,主要有一下三大问题:

2.1.1 匿名环境

现有区块链行业,对于区块链技术应用的核心,仍然围绕着匿名特性,数字加密货币的链上账户与链下真实身份不建立关联,日益成为洗钱、贩毒、走私、非法集资等违法犯罪活动的工具,而相对更为广泛的日常生活应用场景,均需要 KYC 的支持,现有匿名特质的数字加密货币很难大范围落地应用。

2.1.2 技术门槛高

现有区块链行业,基于现有大部分公有链平台,仍无法灵活,快速的构建大众化 Dapp 应用,而底层公有链本身的开发,也具有相当高的技术门槛,需要多

学科学术深度和资源的投入支持。

现在区块链技术所处的阶段与互联网早期阶段非常类似,被一小部分狂热的追捧者所称赞,但在实际应用中由于技术的瓶颈和复杂的操作而很难被大规模使用,因此没有哪个公有链,数字加密货币或去中心化平台已经真正成为社会的主流,中心化解决方案仍然统领整个市场和社会。

2.1.3 资源浪费巨大

工作量证明算法作为区块链第一个也是目前经受住足够实践检验的一个共识机制,解决的是分布式系统交易信息一致性的问题,在一个去中心化的网络中构建了彼此不信任节点的信任机制,也是比特币成功应用的关键技术环节。经过几年的实际运转,这一算法的弊端也显露出来,比特币网络每秒完成 600 亿次 SHA256 运算,消耗了大量的电力资源,而最终这些计算没有任何实际或科学价值,这些运算存在的唯一目的是用来解决工作量证明问题。另外一个现实的威胁便是算力集中,工作量证明本质上是利用穷举法找出符合规定条件的哈希值的过程,算力越强,获得记账权(即挖到矿)的可能性便越高。一开始是最早利用显卡挖矿的人,后来是利用 FPGA 矿机挖矿的人,再后来是利用 ASIC 专用芯片挖矿的人,现在就是不断制造出更好的 ASIC 挖矿的人,另外还有“矿工”节点联合起来组成矿池,如 Ghash 等都在试图不断集中算力。Ghash 2014 年曾经发表声明,将在今后确保不超过 40%的全网算力,这类自律声明是对比特币节点间去信任机制的莫大讽刺。

2.2 区块链行业发展的未来之路

随着大数据时代的到来，越来越多的个人信息和敏感信息被放到了网络上，中心化数据库就像在狼群中的一块肉，随时会成为黑客们的下手对象，近年来的数据库泄露事件已屡见不鲜。区块链技术在未来有可能会成为提升大数据安全机制的一个入口。通过区块链，可以保证不会由于单把私钥的泄漏导致整个数据库的泄漏。以太坊的开发者之一 Roman 认为区块链的最大价值之一是你不能以管理员身份随意改变信息，没人能控制区块链。因此，我们认为虽然目前区块链在大数据安全上的应用还没有非常成熟的案例，但它就像一扇还没有开启的阀门，具有巨大的开发潜力和启发意义。而区块链的去中心化和不可伪造篡改的特性正好契合了这个需求，既能保证数据的安全共享，也能解决数据的归属问题，使数据“取之于民，用之于民”。

总而言之，WISchain 的诞生，将逐步颠覆人们对区块链产品的观念——区块链也可以被普通用户所使用，人人都可以成为区块链产品的拥有者，区块链产品全球化的大繁荣，便指日可待。

2.2.1 区块链产品 WISchain 权威生态圈的构筑

我们的团队具有广泛而且权威的资源，包括全球知名的保险公司，顶尖的网站安全检测评估公司，市场用户调查公司，这些都是构筑权威生态圈的必备优势。将企业网站和个人操作日志等资源进行加密化。结合区块链的不可篡改与可信性，利用 WISchain，简称超级权威，信息安全的数据库。在企业网站进行投保时，我们有一系列的团队一对一专人服务，有针对性的为企业网站设计适合企业的保险，对网站进行实时保险，打造极具权威性的区块链产品生态圈。

2.2.2 挖掘广泛的民间潜在市场

为了打造权威的区块链产品生态圈,可以在我们团队所开发的登录易产品上面,根据用户需求的不同,更换保险内容,让用户有更多可以自己选择的空间,通过使用登录易 APP,使用户接触区块链产品的同时还消除了帐号密码容易遗忘的难题。在 APP 上用户可以选择是否帮助别人存储数据来获得一定的奖励,这种奖励机制一定程度上提高了用户使用的积极性,也为用户带来了乐趣,并且还能更加深刻地了解区块链。

2.2.3 全民化权威区块链产品生态圈

随着平台的推广,越来越多的个人用户,可以通过该平台(登录易)注册个人帐号,该帐号具有唯一性,安全性,保密性;个人用户可以通过登录易方便快捷的登录注册功能省去很多麻烦,而登录易所搭载的 WISchain 极大的保证了用户的帐号密码安全,同时还能扫码快速登录网站。而企业网站用户通过使用我们的 WISchain 保障网站数据库安全或者其他重要机密文件。在保险前期会有专门的团队为企业网站进行安全评估,一定程度上降低了企业网站被黑的概率,并且就算被黑客攻破之后,我们 WISchain 也会根据企业网站的受损程度进行评估赔付,让企业的损失降到最低。随着我们用户群的不断壮大,越来越来的企业使用我们的 WISchain 产品,不仅对企业有益,对于整个中国的网络安全等级都会有一定的提高,社会上所发生数据库,机密文件,隐私泄露的事件会越来越少,达到一种空前的网络安全的繁荣景象,同时更好更快的推动区块链行业的发展,使得区块链不断被大众所认知,所接受。

3 设计理念

针对区块链发展所面临的种种问题，我们提出“WISchain”的概念。设计这个产品的主要目的有两个，其一，对于使用“WISchain”的企业不要通过挖矿来打包数据，而是安全公司打包，这样一样就不会产生因为算力竞争而产生的资源浪费，节约企业成本，其二，不管是企业还是个人用户，对于网站安全还有帐号密码的保护更加安全。网络已日渐成为我们日常生活中不可或缺的一部分。与现实生活中的身份证、护照一样，人们在使用各种网络服务时，如收发邮件、网上购物、网上聊天等，都需要进行网络身份的注册、登录、认证等操作，可以说，网络身份已经成为人们获取个性化网络服务的必备条件。

对网络服务提供保险的想法最早由刘文印博士于 2004 年提出[1-3]。近年来，保险业在网络世界也逐渐获得发展。刘文印博士指出了对网络服务提供保险的重要性及可行的商业模式，涉及了保险公司，安全公司，商业网站和个人用户。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。前者的模式是安全公司售卖安全产品给网站并提供保险，如 360 安全公司。后者则是软件的开发商提供保险，如阿里巴巴公司为支付宝提供保险。不管哪种方式，都需要对购买保险者绝对的信任，因为网络流量数据仅保存在购买保险者一端，而购买保险者可以伪造证据骗保。而且很少有独立的保险公司为网站和软件提供保险，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。区块链保险也开始应用在一些传统行业。阳光保险集团在 2017 年提出将区块链技术应用在航空意外险的购买和理赔。德国的 Etherisc 公司推出了航空延误险、社会安全保险以及农业

险三款试验应用 App。但传统行业的保险仍然存在限制，既理赔证据的数字化和对等性。

3.1 技术目标

3.1.1 主要创新

A) 市场创新：

WISChain 是在一款名为“登录易”的网络身份安全产品的基础上提出的[4]。登录易是一个帮用户（通过扫码）自动注册、登录并管理账号密码的软硬件产品系列，专注解决使用密码时“烧脑”“密码疲劳”等问题，提高上网第一道防盗门的安全性。用户再不需要人工设置、记忆及输入众多密码就能在各种终端上网，既方便又安全。目前，对于大多数网站，登录易还需搭配浏览器扩展插件使用。该产品工作原理是我们独创的基于可信用用户代理的多方闭环网络身份认证机制，颠覆了现有的 B/S 架构用户认证机制但兼容传统账号密码系统，同时可以检测钓鱼和网络非法（包括入侵、后门等）请求。

市场上帮助人们记忆帐号密码的 APP 层出不穷，但是目前现在还没有哪个 APP 使用区块链的技术做帐号保险和企业网站身份安全保险。我们不仅可以帮助用户记忆复杂密码，防止“密码疲劳”、“钓鱼”、“撞库”，同时我们还结合了区块链，保障了用户的帐号密码的安全，为用户登录节省时间，帮助用户节省脑力。对于企业网站来说我们所推出的“WISchain”保险也是企业所需要的，企业有很重要的数据库资料需要我们进行网站安全的保险，一旦发生泄漏或者其他安全事件，可以减少企业的实际损失。特别是 2018 年 5 月 25 日之后，被

有些媒体称为“史上最严数据保护条例”的欧盟《一般数据保护条例》（General Data Protection Regulation，简称 GDPR）正式生效，数据泄露可能会受到高达 2000 万欧元或全球营业额 4%的罚款。GDPR 覆盖范围之广、规定之严、惩罚之重，让企业对于用户数据隐私保护方面空前重视，各大公司纷纷及时更新隐私条例，加强用户数据隐私保护措施，避免受罚。在 GDPR 管制下，由于小公司安全方面不过关，被罚破产的可能性很大。但如果有了 WISChain 的保险作保障，其风险大大降低了。同时，使用我们的“WISChain”进一步减少了用户使用简单密码，被黑客通过用户习惯尝试出密码的可能。

B) 区块链技术创新：

众所周知现在市面上面的区块链产品全部都是匿名化的，这就为那些黑色产业带来便捷，而且由于区块链的特殊性，政府监管的缺乏性，区块链产品不被政府所认可，所以现在区块链 2.0 还是处于一个见不得光的黑色地带。但是“WISChain”的诞生完全消除了大众和政府的顾虑。因为我们采用的是半实名制和半匿名的状态，为什么这么说呢？就是说对于用户来说，用户的身份信息不会通过“WISChain”上链，而是通过用户们的唯一 ID 进行日志的上链，这个 ID 是和用户的真实身份进行绑定的，但是关于身份信息这一方面我们使用一个单独的节点去保存，并且只给政府有查看权限。要是安全问题发生，“WISChain”需要政府的特殊授权才能查看，这样一方面不仅保护了用户的隐私信息和账号安全。另一方面给政府监管的权利，让区块链 3.0 时代可以得到政府认可，让区块链产品成为合法的商品，走进普通大众的生活中，这样就能借用政府的影响力去

推动区块链技术的发展，一定会迎来又一次的网络革新和技术变革的新高潮。

C) 产品技术创新：

区块链是一种分布式系统，其中的存储性能比较差，存储不了大量的数据，但是由于“WISchain”要存储网站的日志，这个日志是实时产生的，要是直接把日志存储上区块链上，这个存储量是非常巨大的。那么要怎么把网站日志存上区块链呢？这里就展现了“WISchain”的技术创新，这里不是直接把日志存储上去，而是把网站一段时间内的日志转换成一个 256 位的 hash 值，这样不仅大大减少了存储量，而且大大节约打包上链的费用。

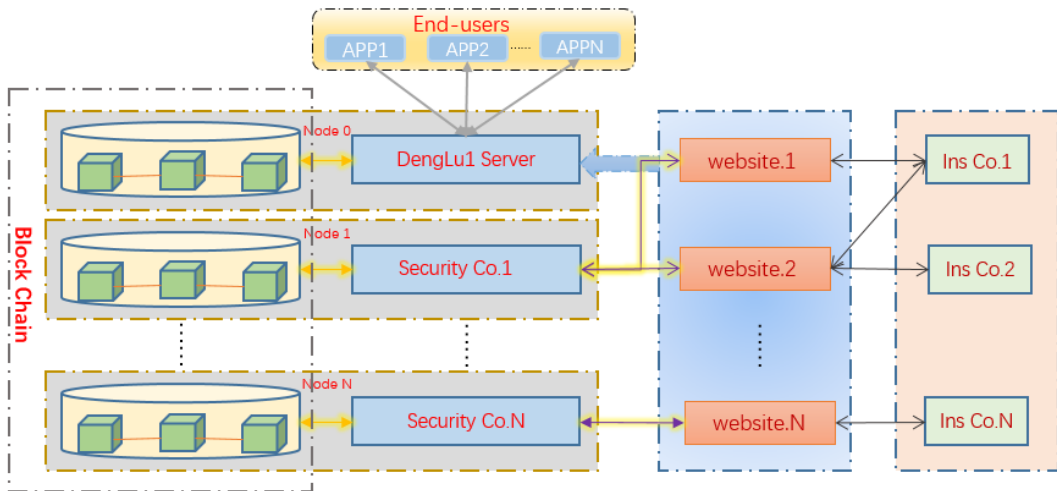
3.1.2 平台模型

首先“WISchain”是基于 parity 钱包搭载的，这个钱包的特点有几个，一个是它因为是重新写的代码，所以跑起来更快，占用系统的资源更少。第二个特点是它的同步功能做得更好，其它钱包往往需要很长时间进行同步，它还是能够很快同步。第三个特点，它虽然是一个全节点钱包，但是它只留下了那些早期区块的区块头，其他内容删减了，所以同步好的区块的大小也就几个 G，而如果是用以太坊的官方全节点钱包，光区块大概就得有 40 个 G。第四个特点，这个对 ICO 特别适用，就是它能够设置定时发送交易，能够在到达某个区块数的时候自动发送转账交易，所以对于“WISchain”的性能来说选择使用 parity 作为平台是最好的。

3.1.3 功能和结构

整体结构：

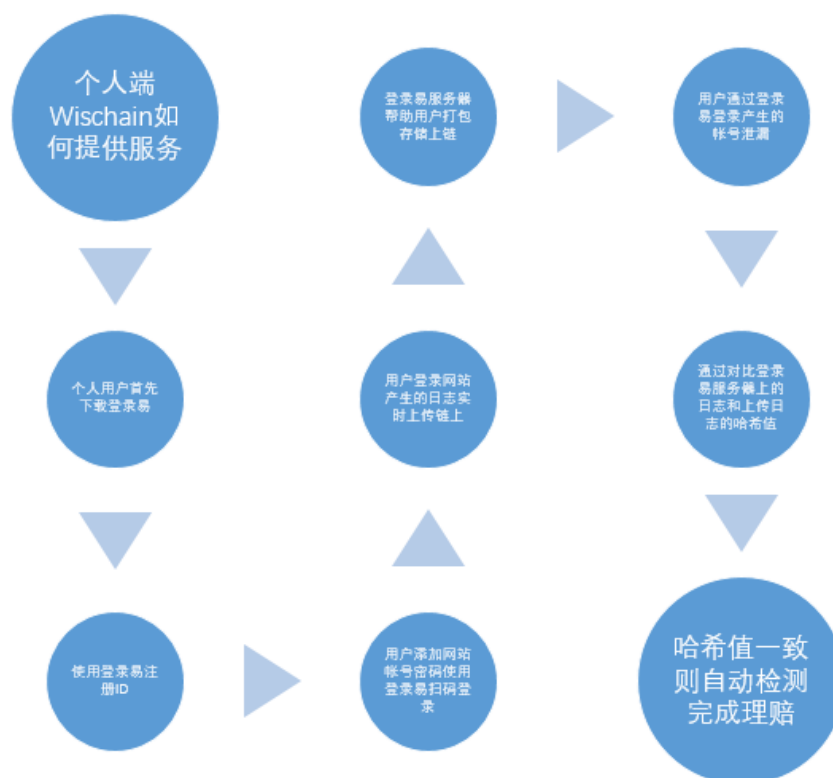
从图 1 可以看出，除区块链作为数据库外，WISchain 包含了五个重要的模块，即登录服务器，保险公司（标记为保险公司 1,2, ... N），安全公司（标为 Sec Co. 1,2, ... N），个人用户（App1,2, ... n）和公司企业网站（Website1,2 ... N）。区块链主要承载最终用户和网站的所有日志的哈希数据。登录服务器和每个安全公司都拥有区块链的完整节点，并负责根据共识机制将上传到区块链的数据打包。每个从保险公司购买保险产品的网站和终端用户都可以聘请安全公司（由保险公司建议）帮助评估网站或他/她的终端访问网站的安全级别。



A) 区块链上的数据：

由于网站上的大量日志和日志的隐私性，日志无法直接存储在区块链中。每个网站每秒的日志哈希数据将由共识机制选择的安全公司上传和打包。确保了日志的安全性和真实性。DengLu1 服务器同样负责上传所有用户日志的哈希数据。

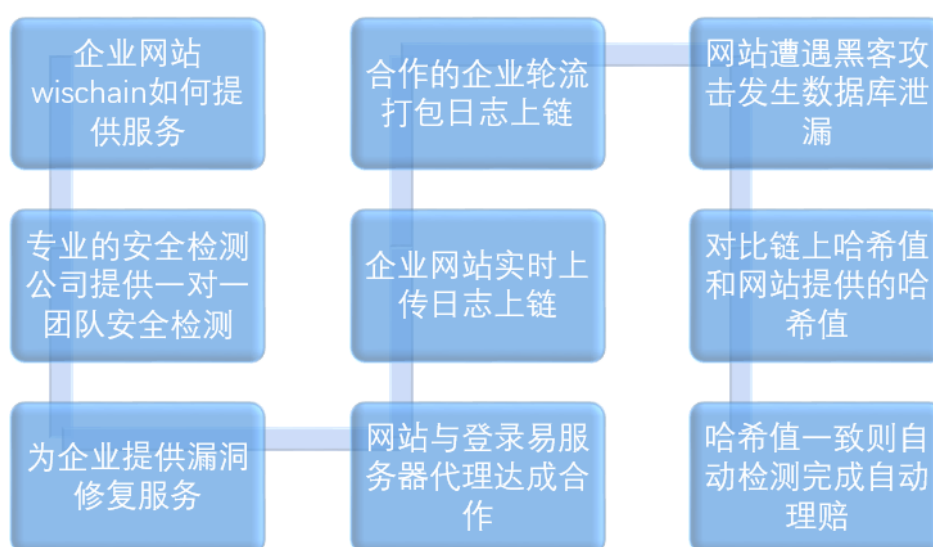
B) 个人用户：



首先个人端需要下载登录易作为一个平台来使用“WISchain”的服务，在登录易里面添加自己的常用网站帐号，配合登录易插件来扫码登录网址。在使用登录易管理帐号时我们可以最大限度的保护我们的信息泄露，信息泄露的方式大致有三种：撞库/爆破（撞库：黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。爆破：黑客尽可能地尝试所有可能的密码，直到登录成功为止），钓鱼攻击（钓鱼式攻击是一种企图从电子通讯中，通过伪装成信誉卓著的法人媒体以获得如用户名、密码和信用卡明细等个人敏感信息的犯罪诈骗过程），以及社会工程学（社会工程学是一种黑客攻击方法，需要搜集大量相关的信息，利用欺骗等手段骗取对方信任，获取密码等隐私内容的）。个人的网络身份信息（账号密码）是我们

的重要保险对象。个人参与 WISchain 的保险业务建立在使用登录易的基础上，用户使用登录易管理他们想要保护的账号密码和对任意的账号密码购买保险，而且所有的注册、登录和修改密码等操作都通过登录易。登录易将用户的操作日志记录在区块链上。若用户的账号密码被非法手段偷窃，用户能获得保险赔偿。

C) 企业的网站：



对于企业网站来说，首先企业向“WISchain”发出想要合作的意愿，并由“WISchain”的合作对象安全检测公司去给企业网站进行漏洞检测，并由企业决定是否进行修复，根据网站的安全评级来划定保险金额。要是在保险期间企业网站发生黑客攻击，发生数据泄露，根据泄漏的等级来理赔保费。但是由于网站内部所造成的损失，“WISchain”不给与理赔。其中要是有出现骗保或者欺瞒等行为，“WISchain”保留法律追究责任。以淘宝网站为例，淘宝会员的帐号密码属于重要资产，当帐号密码发生泄漏时，一定会产生会员的资产损失，这时像淘宝这样的公司可以和 WISchain 合作，可以将所有的项目条款预先确定为智能合

约。如果会员的账号密码在企业端发生拖库，导致数据库泄漏，企业可以上传泄漏账号凭证，合格的第三方将对其进行检查并处理索赔。当约定事件触发索赔时，智能合约将自动处理付款和报销。链上的时间戳可用于验证事故的有效性。更重要的是，商业网站为他们的网站数据库进行投保，会在同行间提升竞争力，这使得他们比没有投保的网站更能获得用户青睐，而且不用担心数据泄露所带来的损失。

D) 保险公司：

对于各种应用场景的保险需求的不同，保险公司将推出各种不同种类的保险。保险公司的服务对象可以分为两类：第一类是使用登录易的个人用户，保险公司允许用户自己设计保险类型（特定的帐号密码），用户发表自己的个性化需求之后，与 WISchain 合作的保险公司将对需求进行估算，包括价格，预期利润和潜在风险，给用户设计一个个性化的保险方案，再由用户自己决定是否使用此保险公司提供的保险方案。第二类是企业网站，保险公司对商业网站的保险重点在网站的数据库。同样，企业可以根据网站数据库的重要程度不同来选择不同的保险公司和不同保险业务。我们有完整的符合经济学的购买保险费用和赔偿金额的设计。实际上，大多数基于情景的保险都可以采用智能合约的方式达到自动快速赔付。在复杂保险赔偿问题上，安全公司作为主要评判人，根据用户的具体出险情况和网络日志证据做出裁决。用户也能够上传相关材料，并且材料将被交叉检查并记录在链上。

E) 安全公司：

在企业网站需要投保时，安全公司对网站进行全面的安全检测，提高网站的安全等级并且降低出险率。在理赔复杂的企业网站的保险时，安全公司可以作为中立的评判者来检测网站的攻击是否属于理赔范围。安全公司打包网站日志，将会得到一定的代币奖励，这个代币可以用来购买和 WISchain 合作企业的产品。

F) 登录易服务器：

登录易服务器是 WISchain 的一个关键组件，它是所有终端用户在用于注册/登录/修改时所有 Web 身份的中心。它会记录其哈希值上传到区块链的所有日志，以便在提出索赔时检查保单持有人向保险公司提交的日志的真实性。

4 共识机制 POA (Proof of Authority)

4.1 普通的 POA

所谓权威证明 (PoA)，就是使用一组所谓的“权限”来允许人们在区块链上创建新的节点并确保区块链的安全。以太坊测试网 (Kovan) 便是采用 PoA 算法。

在 PoA 中，验证者 (validator) 是整个共识机制的关键。验证者不需要昂贵的显卡，也不需要足够的资产，但验证者必须具有已知的，并且已获得验证的身份。验证者通过放置这个身份来获得担保网络的权利，从而换取区块奖

励。若是验证者在整个过程中有恶意行为，或与其他验证者勾结。那通过链上管理可以移除和替换恶意行为者。现有的法律反欺诈保障会被用于整个网络的参与者免受验证者的恶意行为。

通俗的理解就是，以前我们交易需要一群互不认识的人来拼算力，艰难的计算一道复杂的数学题，从而争出个输赢。而现在，我们只需要有一个信得过的人（至少得到了他们团队的认可）做担保，便可快速通过交易。而这个人也会因为这笔交易做担保，而获得报酬。要是这个担保人使坏怎么办？没关系，其他的可信担保人看着呢，他要是敢使坏，我踢你出局。而要是担保人故意为难你呢？没关系，现有的法律可以保证你的合法权益（注意，数字资产丢失不在我国法律保护范围）。

4.2 POA 与代理权益机制的区别(DPoS)

DPOS 通过使用见证人产生区块来运行。见证人是被利益相关者选举出来的，选举方法是一票一个见证人一份权益。然而，在 POA 中，权威的指定是事先钦定的，这意味着不会由于不公平的权益(Stake)产生偏见和不公平的过程。在 POA 中，见证人需要用他们自己的身份通过 Dapps 正式验证，并且在公开的领域他们的身份信息对每一个人都是透明可见的。

4.3 POA 的优势

POA 背后的理念是个人或组织、机构争取去成为见证人的权利，因此他们有保持自己原有地位的激励。通过把身份和声誉绑定在一起，见证人被激励去

验证交易和维护网络安全，他们不会希望把自己的身份和一个不好的声誉联系在一起。这个机制被认为比普通的权益证明机制（POS）更安全。

4.4 WISchain 的 POA

WISchain 在传统 POA 共识机制的基础上做出了改良，传统的 POA 是一些“权威”进行打包，这样那些想干坏事的“权威”节点可能联合勾结在一起，去破坏网络安全，由于 WISchain 的特殊性，可以将“权威”节点变得不再权威，之前权威节点的打包任务，现在可以由 WISchain 的合作方，多家安全公司来进行打包，这样可以有效地防止企业网站在对自己的日志打包上链时进行篡改，恶意骗取保险的行为。WISchain 使用 parity POA 作为共识机制。WISchain 还希望建立一个分散的，点对点的保险市场来欺诈，这在保险业中很常见。我们还使用信用/代币机制来奖励那些有信誉的保险公司和那些做出其他贡献的人，例如数据打包者。该奖项可用作奖励，以激励用户维持可持续发展系统的良性循环。

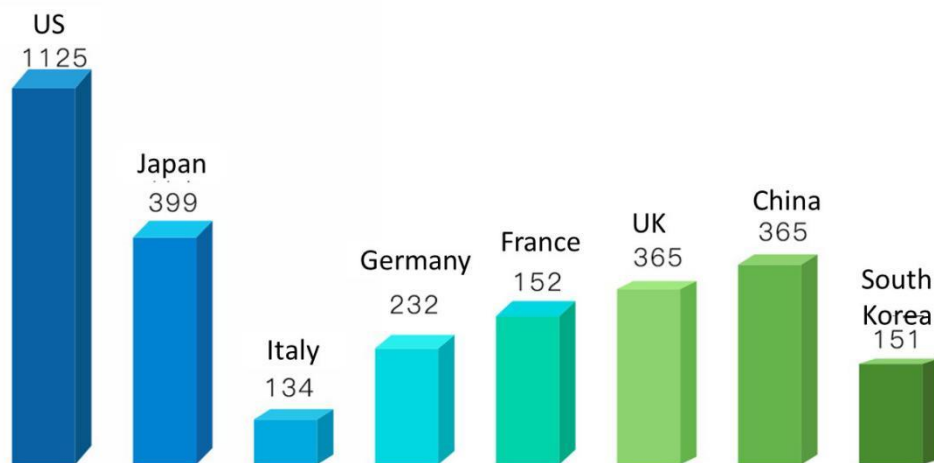
5 保险市场和应用场景

5.1 保险市场

5.1.1 市场潜力

保险业是一个巨大但发展迅速的行业，具有无限的市场潜力。全球保费收入为 4.8 万亿美元。随着经济的发展，全球保险需求迅速增长。根据 2017 年全球保险评估以及 2018 年瑞士再保险的展望，2018 年世界经济将保持稳定增长，

保费也将保持稳定增长。2017 年和 2018 年全球非寿险保费分别增长 2.2% 和 3.0%。全球人寿保费分别在 2017 年和 2018 年分别增长 4.8% 和 4.2%。新兴市场，特别是亚洲的新兴市场将成为保费增长的推动力。2017 年上半年，中国的保费收入达到 2.31 万亿人民币（3.6 亿美元），与去年同期相比增长了 23%。



Premiums in 2016 (billion Euro)
Data from Allianz World Insurance Market Research

5.1.2 市场挑战

虽然保险在全球范围内仍然发展迅速，但其发展遇到了诸多挑战。保险面临的主要挑战如下：

A) 太多的中介：

传统保险高度依赖中介。大部分溢价已用于支付渠道成本，客户无法适当投保。

B) 缺乏数据保护：

保险公司拥有大量的客户数据，包括私人数据，如政策信息，家庭成员

和电话号码。保险公司在保护客户隐私方面并不认真，导致客户隐私泄漏。

C) 营销误导：

在试图说服消费者购买他们的保单时，保险代理人或销售人员说谎或扣留信息。这已经损害了消费者的权利以及保险的声誉。

D) 缺乏创新：

大部分保险公司提供的政策在各方面都相似。它可以解决消费者面临的某些问题，但不能满足所有个性化需求。

5.1.3 市场机会

所有这些挑战都可以在区块链的帮助下解决。区块链是一种分布式账本技术，具有透明性、可追溯性和不可伪造性等特性。所有这些功能都完美匹配保险的性质。通过利用区块链，保险公司将能够通过连锁收集消费者的数据，而不需要他们重复提供材料，智能合同可以在索赔过程中替代人工，并且可以防止所有欺诈行为。区块链上的所有交易都将被永久记录并可追溯，因此它可以帮助保险公司准确地分析每位客户并提供个性化定价。

在保险领域里面的应用，这个可能会更快一些。因为现在保险的基本数学模型太落后了。我们现在的数学模型，大家如果对保险行业了解的话，知道是大数定律，那个模型是一百年前的东西。我们现在都到什么时候了，我们信息量跟一百年前比起来，已经远远不是那个时候的样子。所以在这个情况之下，保险模型一定要发生改变。这是一个因素。

还有一个很重要的原因，那就是保险的发展空间太大了。我们现有的保险产

品不是太多了,而是太少了 根本满足不了我们的需要。区块链保险太有价值了。如果我们能用区块链重新设计它,那么这个价值将会非常巨大。它是既填补了以前的空白,又能够去颠覆这个产业的基础的数据模型。区块链将成为下一代保险的基础技术和促进保险发展的引擎。基于区块链的保险将成为该行业的重要组成部分,甚至可能重新定义保险。

5.2 应用场景

在网络身份安全保险中,主要可以分为两个场景:个人终端用户和企业网站。无论是个人还是网站,信息的安全都是至关重要的。当今网络安全形势情况下,我们力求找到一条最合适的渠道,将网络身份安全保险的效果发挥极致。对于个体终端和企业网站,网络身份安全保险的应用场景不尽相同,接下来我们将对这两者各自做一个简单的讨论。

5.2.1 个人终端用户

随着网络更好更快的发展,个人用户网站的帐号越来越多,这时就会出现一些帐号密码被遗忘的烦恼。这个时候就会需要一个辅助工具来帮助我们记忆帐号密码,虽然传统的手写方式也可以帮助我们记住帐号密码,但是这样的方式不仅效率低下,而且一旦手写的帐号密码丢失,被心怀不轨的人捡到,可能会有帐号被盗的风险,造成严重的财产损失。于是我们可以借助使用登录易帮我们管理帐号密码,并且可以配合插件使用扫码功能快速登录网站,同时使用登录易的用户可以享受“WISchain”的保险服务,在使用登录易扫码登录期间被其他人窃取帐号信息所造成的财产或者其他实质性损失,用户可以通过登录易 APP 进行线

上申请理赔,提供一些证据截图或者记录传送给后台,后台使用人工智能技术自动验证其证据的真实性,一旦泄漏属实,理赔金额即时到账(保留人工核实功能,一旦发现骗保或者其他异常,我们将启用法律的手段追究用户责任)。

5.2.2 企业网站

以淘宝网站为例,淘宝会员的帐号密码属于重要资产,当帐号密码发生泄漏时,一定会产生会员的资产损失,这时像淘宝这样的公司可以和 WISchain 合作,可以将所有的项目条款预先确定为智能合约。如果会员的帐号密码发生泄漏,会员可以上传泄漏帐号凭证,合格的第三方将对其进行检查并处理索赔。链上的时间戳可用于验证事故的有效性。当一个企业网站为他们的网站数据库进行投保,会在同行间提升竞争力,比起没有投保的公司,更能吸引用户去使用、成为网站会员,而且不用担心数据泄露所带来的损失。

5.4 WISCHAIN 生态圈的建立

我们计划建立一个基于区块链的保险生态系统,每个用户都可以设计,购买和投资保险,提供各种网络安全信息,包括新发现系统安全漏洞、黑客攻击情报等。这个生态系统将能够满足客户需求,并对那些提供有用情报、信息、创意和创新的人提供奖励,消除传统保险中的中介,降低运营成本。

6 WISCHAIN 基金会

WISCHAIN 基金会旨在为加入 WISCHAIN 的所有用户,提供一个独立、非

营利、民主的治理机构。

6.1 WISchain 基金会的主要职责

基金会将囊括互助组织、公证机构、爱心机构、其它互联网组织等（以持有大量的代币为基础），对平台资源进行开放式管理（包括市场推广、底层服务体系搭建等），大力支持和推进与平台相关的技术发展，维系 WISCHAIN 创建机制，以及升级整个生态的风险控制体系。

WISCHAIN 的高效运转，将吸引更多的用户加入平台，挖掘平台对自身的服务价值，以开发、服务和吸引用户为工作目标。随着时间推移，基金会将更加趋向于去中心化自治组织，建立正式的运转规范和运营标准。

6.2 WISchain 基金会的发展目标

发展底层技术和应用工具，对所有参与者逐步实现友好的机器语言和交互界面，使更广泛的开发者和维护者，进入整个生态，维护一套开源代码库，加强平台的运转效率和稳定性。

发展自治社区文化。互助生态，将使用户的关系更加紧密，用户在同一社群中，通过沟通加深互助精神，从而发挥群体智慧，对生态系统进行进一步优化，让所有参与者更好地从中受益。

6.3 WISchain 基金会治理目标

研究公平、透明的治理规范和标准，深切考虑所有参与者、用户的共同利益，达到对各方推进和制约的双重效果，实现多方共赢的最终目标。研究稳定、高

效的市场体系，包括各互助群体的推广和范围界定，风险系数的核算，WISCHAIN 的创建和流通，公证组织的权限和协议等。研究风控模型和经济模型，保证超大规模的经济网络可以长久的运行，不受经济危机、通货膨胀等金融风暴造成创伤性危害。

7 发展路线图

7.1 合作伙伴

WISchain 以开放包容的形态以及共同一致的愿景，吸引全球的互助机构、互助保险公司、其它互联网组织，成为 WISchain 的合作伙伴。合作伙伴的共同点是：以用户互助为主要实现方式，以解决网站保障及身份安全保障为运营目标。由于市场、运营的侧重点不同，各合作伙伴可以在社区中起到不同作用，实现广泛意义上的共赢和资源共享。

7.2 竞争对象

对于“WISchain”来说所有的传统的保险行业都是其竞争对象，但是前期也是合作伙伴。“WISchain”冲击了传统保险行业，不仅效率是传统保险行业的几十倍。但是随着“WISchain”用户的不断壮大，这些竞争对象也会逐渐变成合作伙伴，推动社会经济的快速发展。

7.3 项目风险

7.3.1 市场风险

市场风险是指项目没有被市场接纳，或者没有足够用户使用，业务发展停滞，WISCHAIN 市场参与者不足。

针对市场风险运营团队采取的避险方式为：经过多年的市场实际运行经验，确认市场痛点客观存在，不断与业界分享 WISCHAIN 理念，借鉴同类产品运营经验，对 WISCHAIN 优化改进，并利用创始团队在保险市场服务中积累的经验，迅速吸引项目初始用户。

7.3.2 技术风险

技术风险是指底层技术出现重大问题，导致项目无法实现预期功能，以及关键数据被篡改或丢失。

针对技术风险运营团队采取的避险方式为：基于成熟、开源、安全的区块链技术，采用已经被大量用户使用和长时间稳定运行验证过的架构开发系统。

8 团队及主要成员介绍

团队创始人：刘文印

刘文印博士现为广东工业大学计算机学院特聘教授及广东省引进创新团队带头人，博士生导师，国际模式识别学会会士，是国际上反网络钓鱼式欺诈 (Anti-Phishing) 领域的先锋之一、国际模式识别领域的知名专家，发表论文300多篇，

h-Index指数为45，发明近20项专利技术。

刘文印博士于1988年和1992年分别获清华大学计算机系工学学士和硕士学位，1992年留校任教，1995年赴以色列理工学院(Technion)留学，1998年初获博士学位，1999年1月加入微软中国研究院任研究员，2002年1月加入香港城市大学电脑科学系，任助理教授及博士生导师，2015年入选广东省第五批引进创新科研团队带头人，创立网络身份安全实验室，致力于研发国际领先的网络身份安全技术，包括准确验证和便捷管理网络身份，及防止身份造假、假冒、欺诈、泄露、被盗等。刘文印博士因在图形识别及反网络钓鱼欺诈等研究领域的杰出贡献，于2010年入选国际模式识别学会会士 (Fellow of IAPR--International Association for Pattern Recognition)，因在图形识别等研究领域的突出贡献，于2003年获国际模式识别学会颁发文档分析与识别领域杰出青年科学家奖 (IAPR/ICDAR Outstanding Young Researcher Award)。2018年开始定期在微信公众号“登录易”发表网络身份安全及区块链方面的原创科普短文。刘文印博士也是天使投资人，投资领域包括网络安全、区块链、互联网+、大数据及机器人等。

团队成员：吴鸿文

前腾讯互娱高级工程师，深圳青番茄文化传媒有限公司 CTO\架构师。目前在广东工业大学计算机学院就读硕士学位，是“WISchain”的第一批参与者。

团队成员：郭玉荣

目前在广东工业大学计算机学院就读硕士学位，是“WISchain”的第一批参与

者。

团队成员：冼祥斌

目前在广东工业大学计算机学院就读硕士学位，是“WISChain”的第一批参与者。

团队成员：陈佳伟

目前在广东工业大学计算机学院就读硕士学位，是“WISChain”的第一批参与者。

参考文献：

- [1] Liu Wenyin, “Insurance of Business Web Services—A New Business”, Proc. KEST 2004 - Second International Conference on Knowledge Economy and Development of Science and Technology, September 17-20, 2004, Beijing, China, pp. 485-491.
- [2] Liu, W & Liu, A & Li, Q & Huang, L. (2010). Business models for insurance of business web services. Service Intelligence and Service Science: Evolutionary Technologies and Challenges. 261-272. 10.4018/978-1-61520-819-7.ch014. (Liu W, Liu A, Li Q, et al. Business models for insurance of business web services[J]. Global Business Concepts Methodologies Tools & Applications, 2011.)
- [3] An Liu, Liu Wenyin, Liusheng Huang, Qing Li and Mingjun Xiao, “Insurance-Based Business Web Services Composition”, International Journal of Organizational and Collective Intelligence (IJOICI) 1(2), 2010 |Pages: 16, DOI: 10.4018/joci.2010040104 (Intelligent and Knowledge-Based Computing for Business and Organizational Advancements, 2012, pp. 157-173, DOI: 10.4018/978-1-4666-1577-9.ch009)
- [4] Yurong Guo, Zongcheng Qi, Xiangbin Xian, Hongwen Wu, Zhenguo Yang, Jialong Zhang, Wenyin Liu, “WISChain: An Online Insurance System based on Blockchain and DengLu1 for Web Identity Security”, Proc. 2018 IEEE International Conference on Hot Topics in Information-centric Networking (IEEE HotICN 2018), Aug 15th-17th Shenzhen, P.R.China

附件：

“WISChain: An Online Insurance System based on Blockchain and DengLu1 for Web Identity Security”