**Mutual Chain**

**A High Performance Blockchain Framework for Mutual Financial Service**



**White Paper**

**August 2017**

|  |  |
| --- | --- |
| Author(s): |  |
| Version: | 1.0.0 |

AMENDMENT HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Editor** | **Changes** |
| V0.1 | Jun. 25, 2017 | W. QIN | 1. Initial version |
| V0.2 | July 6, 2017 | Gavin Zheng  X. Tang | 1. Add Chapter9 about smart contract 2. Mutual Insurance logic diagram added |
| V0.3 | July 8, 2017 | Z. He | 1. Add blockchain values for insurance to section 2.1 2. 3 Insurance use cases |
| V0.4 | July 15, 2017 | W. QIN | 1. MChain Value Network, |
| V0.5 | July 22, 2017 | W. QIN  Gavin Zheng | 1. MChain Middleware |
| V0.6 | July 29, 2017 | W. QIN  Sean Tang | 1. Fintech Engine 2. Insurance Business Logic |
| V0.7 | July 30, 2017 | DavidCao | 1. Content Update |
| V0.8 | July 31, 2017 | W Cai | 1. Structural Change 2. Added Insurance concept 3. Moved cumbersome insurance user case to appendix, main body only discussed the framework |
| V0.9 | Aug. 8, 2017 | Sean Tang | 1. Mutual Insurance Sample |
| V1.0.0 | Aug. 13, 2017 | W. Qin  Leon. Liu  Jie Lan | * Leon Liu version added, more for IMG * Jie Lan provided the English translation partially * Wenyan updated and integrated into new version |

* **CONTENTS**

1 概述– 基于加密数字货币的互助金融解决方案 5

1.1 背景介绍和互助链的使命 5

1.2 互助区块链的构成与特征 5

2 Mutual Chain系统构架 9

2.1 Mutual Chain的商业工具 9

2.2 Mutual Chain链式结构 10

2.3 Mutual Chain系统实现 – 数字资产计算理论设计原理 12

3 应用场景分析及流程架构 13

3.1 保险应用场景角色概述 13

3.2 互助保险应用承保逻辑 16

3.3 互助保险应用理赔逻辑 17

4 互助链区块链浏览器与钱包 19

5 互助链区块链中间件构架 20

5.1 互助链跨链价值网关 21

5.2 互助链Fintech引擎 21

6 互助链智能合约逻辑 21

7 互助链数字资产与交易 21

8 互助保险系统 24

8.1 为什么选择以太坊 24

8.2 智能合约平台 24

8.3 系统框架 25

8.4 互助币 25

8.5 人工智能模块 26

8.6 风险防范 26

9 互助链应用实例：一个互助保险的说明 29

10 互助链Muton币ICO及ICO之后的项目情况 31

10.1 互助币Muton（代币符号:MUC）的发售 31

10.2 互助币的锁定机制 31

10.3 互助币最低筹集资金和资金使用情况 31

11 互助链开发计划与预算 31

12 互助链团队 31

13 附录 31

13.1 其他应用场景详述 31

13.1.1 互助链架构应用于保险流程的优化 31

13.1.2 互助链架构应用于房屋贷款审批及投资平台 36

13.2 项目组织结构 37

13.2.1 核心团队 37

13.2.2 角色与责任 38

13.3 主要里程碑Key Milestone 38

# 概述– 基于加密数字货币的互助金融解决方案

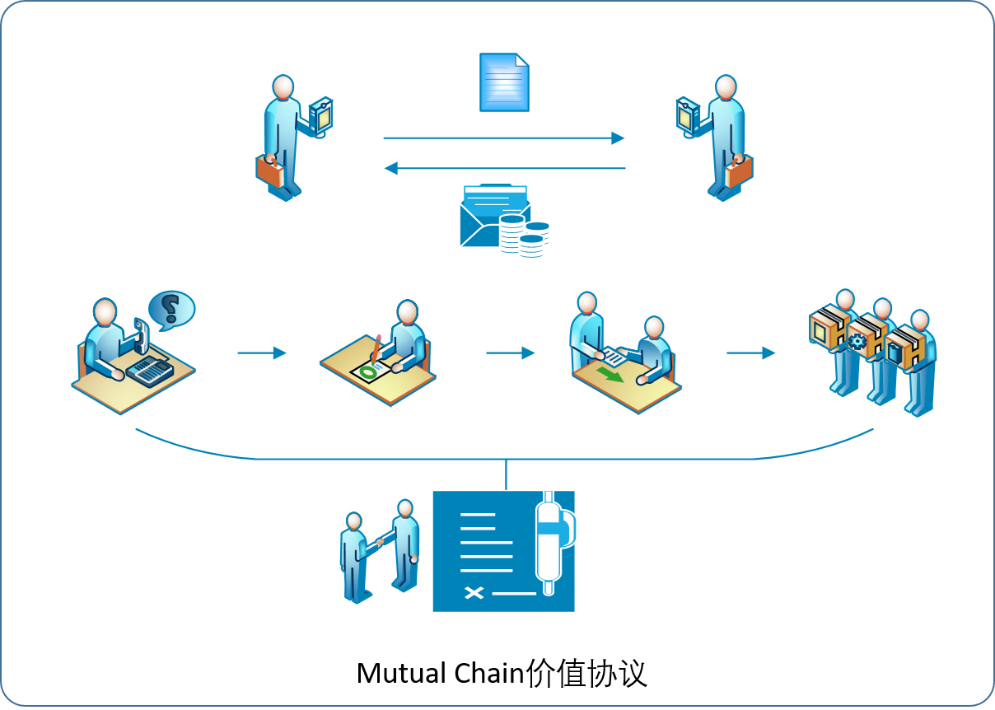
互助链（Mutual Chain）是一个基于加密数字货币的互助金融技术构架和完整的（金融）产品及服务的解决方案， 是全球独创作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成金融应用，旨在打造一个全球化分布式网络自主，共赢，共享的社会化运转机制。虽然区块链技术还处于发展的初期，但其更加透明、开放的理念和机制已经展现出无比的生命力，同时以比特币、以太坊为代表的数字货币的出现正在以燎原之势震动着传统的货币体系和金融体系。互助链正是这一基础上，建立一个分布式的未来个人金融中心，同时逐步发展成为一个分布式的数字资产金融基础设施网络。

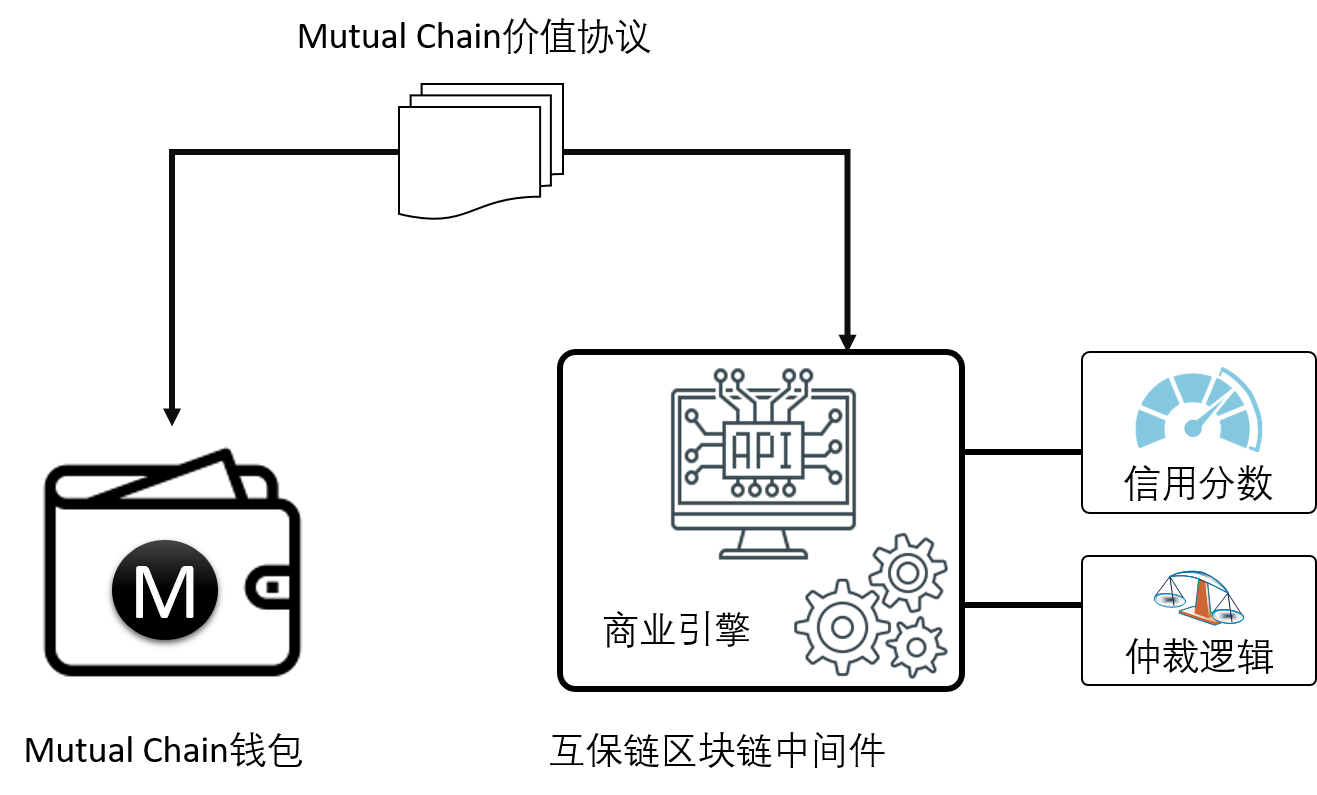
## 背景介绍和互助链的使命

互助链（Mutual Chain）的使命是使每一个人都能轻松的启动和支持创建全新的基于数字货币的新金融服务和产品的项目。通过互助链，任何机构和个人，都可以在未来互助链中开设自己的业务窗口，拥有自己的数字钱包和自己的互助链信用体系，同时互助链提供特有的仲裁机制，一旦产生争议，仲裁机制将对交易内容和历史进行分析，提供仲裁依据和帮助。通过互助链提供的基于区块链的商业工具，现代社会中的商业模式和金融服务可以更加快捷高效的融入互助链引擎中，并且建立各自的金融服务区，使得更多人能够享受更加丰富的基于数字资产的金融服务， 比如保险，个人信贷等等。更加准确的描述，互助链是一个基于区块链的分布式超级金融产品及服务市场。

## 互助区块链的构成与特征

互助链（Mutual Chain）由互助链价值协议与互助链价值网络组成。互助链价值协议包括钱包，信用度和仲裁机制。互助链钱包提供给个人或者机构存贷、兑换、支付、结算等服务，使得互助链链中的金融产品可以通过钱包进行交易和服务。 同时互助链信用度通过交易和链中行为积累，维持整个互助链交易信用体系。仲裁机制监督所有交易和执行，并对交易历史和数据进行分析，产生仲裁依据。





互助链价值网络由金融服务区和商业逻辑组成，通过区块链底层协议将互助链参与的一切交易数据真实源记录通过验证数据分享的开源机制写入到各个节点中,让真实数据通过智能合约变得更加简单而可靠,让每个人在商业活动中都能成为自己的智能合约执行者和数据分享者,并通过共同数据验证机制保证交易的安全和可靠性, 我们通过区块链的共享和写入机制,形成一个平行于现实世界的可调用,可验证的真实区块链金融网络.



在技术实现上，区块链的底层协议将保证数据的公正，安全和可靠。狭义来讲, 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构, 并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。它具有以下特性，

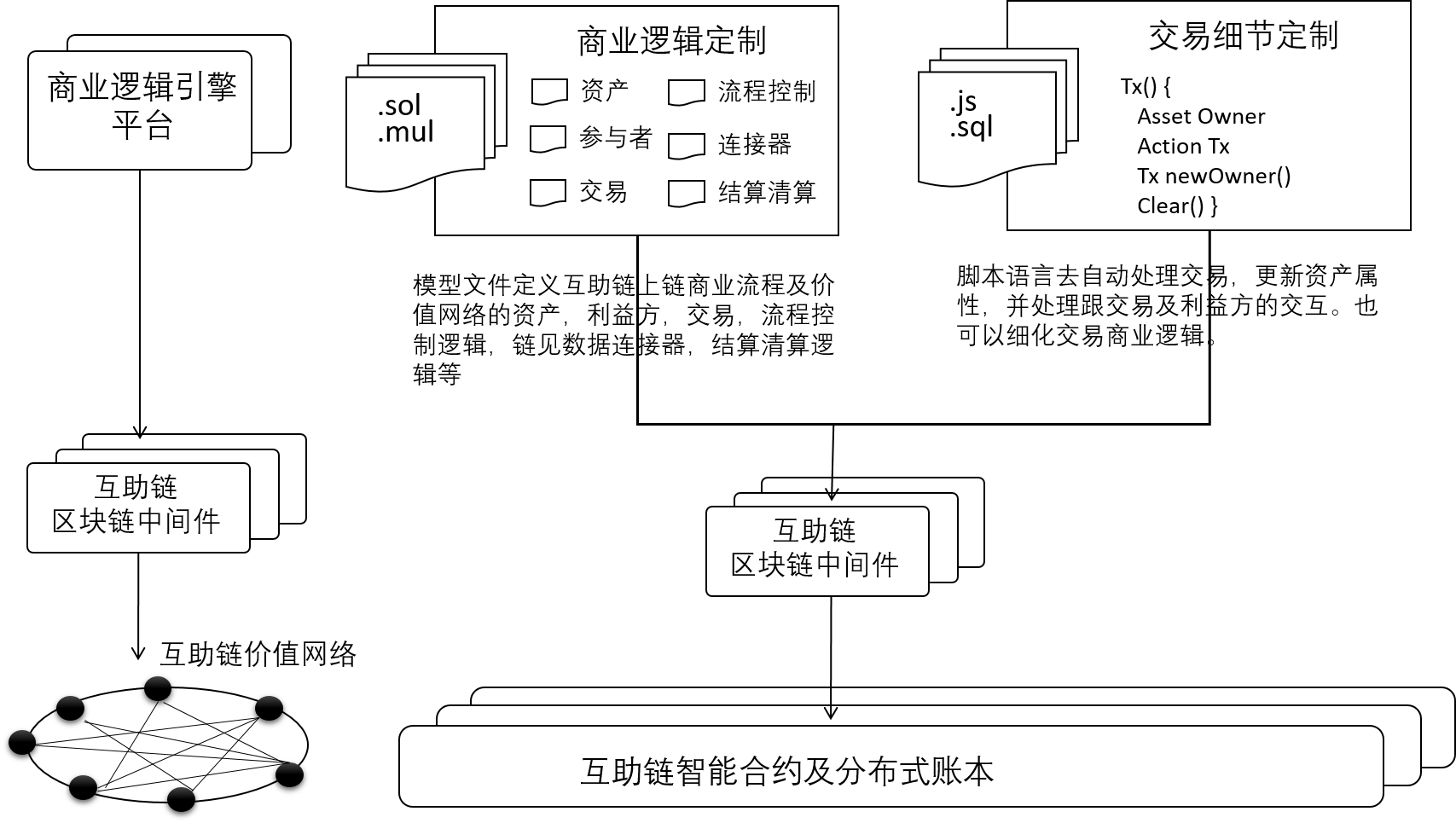
1. 区块链网广播 ( Broadcast )，以区块为单位的链状数据块结构：区块链系统各节点通过一定的共识机制选取具有打包交易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发生的有效交易及其梅克尔树根值等内容打包成一个区块，向全网广播
2. 全网共享账本（SharedLedger）：在典型的区块链网络中，每一个节点都能够存储全网发生的历史交易记录的完整、一致账本，即对个别节点的账本数据的篡改、攻击不会影响全网总账的安全性。此外，由于全网的节点是通过点对点的方式连接起来的，没有单一的中心化服务器，因此不存在单一的攻击入口。同时，全网共享账本这个特性也使得防止双重支付成为现实。
3. 源代码开源：区块链网络中设定的共识机制、规则等都可以通过一致的、开源的源代码进行验证。
4. 非对称加密：典型的区块链网络中，账户体系由非对称加密算法下的公钥和私钥组成，若没有私钥则无法使用对应公钥中的资产。
5. 智能合约 （SmartContract）：区块链系统中的应用，是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。
6. DAPP：包含用户界面的应用，包括但不限于各种加密货币，如以太坊钱包。互助链将发行自己的代币用于链中的金融交易。
7. 虚拟机：用于执行智能合约编译后的代码。虚拟机是图灵完备的。

# Mutual Chain系统构架

## Mutual Chain的商业逻辑引擎

平台将以互助和对等方式，让用户可以建立自己的金融产品和网络，发起人可以通过平台提供的模板快捷的建立可流通的金融协议，比如保险产品，信贷协议，期权等等。发起人可以指定参与方或者公众发售。同时发起人定义协议的执行方式，以保证参与各方的利益。 一旦完成，这款协议可以作为金融产品应用到互助链中，并通过互助链公告板发送给公众或者指定方。如果有用户参与，金融协议即刻 绑定参与者以智能合约形式进行流通和执行。平台工具包括：

1. 资产定义(Asset Definition)： 发起人可以定义互助链流通资产和金融协议。对于保险业来说，发起人可以设计一款保险产品的属性和内容作为链中流通资产。
2. 参与人定义(Participant Definition)：发起人定义协议或者产品的参与方，可以是对公众，群体或者互助链中的个人发售。
3. 接入控制(Access Control): 虽然共享账本，发起人可以定义各个参与方的访问权限。
4. 核心交易(Core Transaction): 金融产品或者协议的执行方式，这是各个金融产品在互助连中的核心交易流程以及保证，以智能合约的形式在互助链中执行。
5. 共联(Connector)：这是各个金融商业区的企业级整合工具，通过共联可以实现链数据和现有中心商业网络的互联和整合，建立一个区块链和中心金融服务区的混合应用。



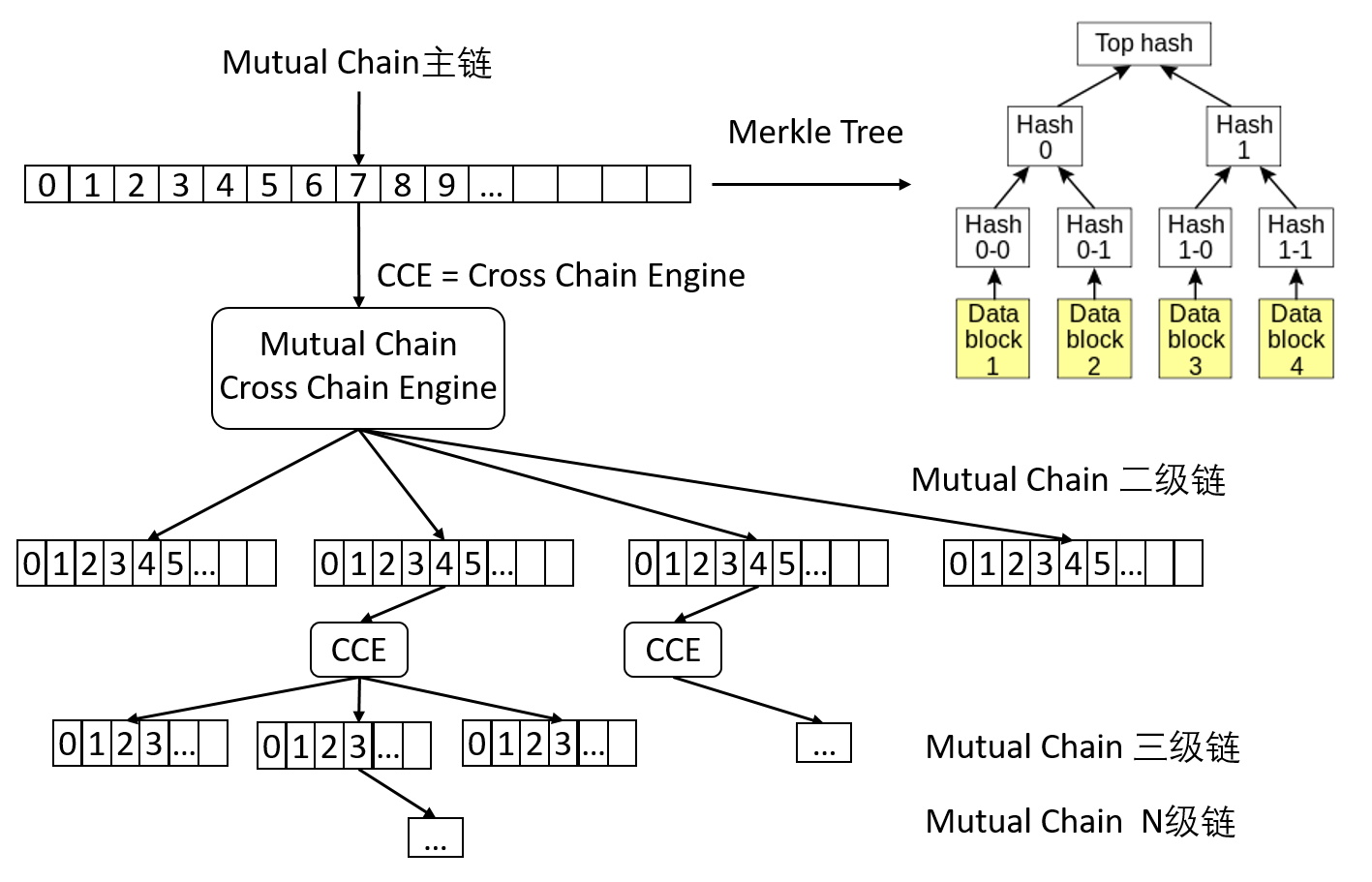
## Mutual Chain的区块链中间件

Mutual Chain区块链中间件是帮助企业和商业用户创建，设计，定制，运营自己的互助链而使用的企业级区块链应用产品。在价值网络搭建起来并运营后，当一个完全的去中心化方式的价值网络不一定需要区块链中间件就能自己存在，但是大量的企业用户回因为有区块链中间件而大大的降低研发和运营成本，提高价值网络流转效率。

## Mutual Chain链式结构

Mutual Chain是一个松紧耦合可配置的复杂多级链式结构

* 用户和系统可根据业务场景需要在部署前进行调配(configurable)
* 多级链式结构间通过跨链引擎来协调与复制/同步
* 链间连接通过加密HASH函数保障安全性，可扩展性和可访问性



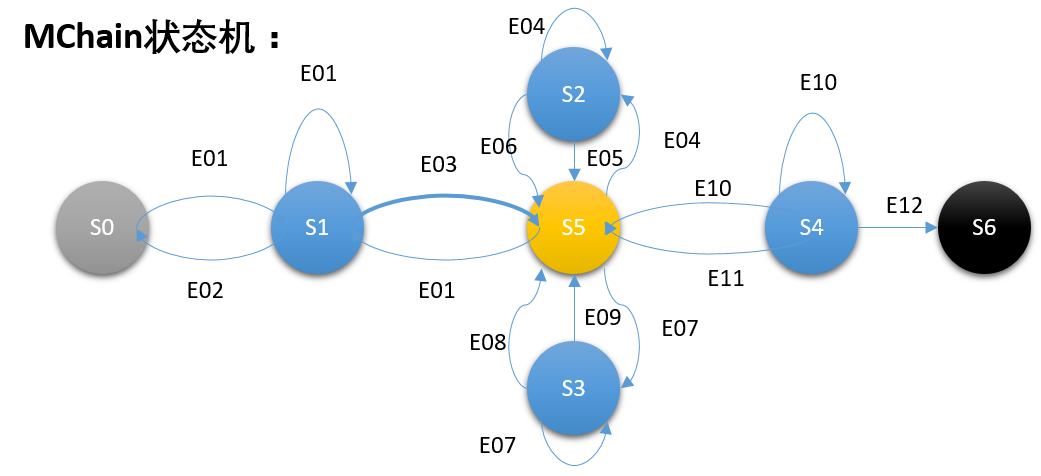
## Mutual Chain系统实现 – 数字资产计算理论设计原理

（Mutual Chain状态机）确定型有限状态机原理理论描述：

Mutual Chain上链信息是一个确定型有限状态机 - Deterministic Finite State Machine (DFSM)

**M=(Σ,S,s0,δ,F)**

* Σ是输入字母表 (有限，非空）- 动作
* S是有限非空状态- 状态(目前暂定5个状态)
* s0是初始状态S的一个子集
* δ是状态转换函数：δ：S x Σ -> S (δ必须返回一个属于S的状态s)
* F是一组最终状态集，是（可为空）S的一个子集



**MChain状态转换函数（区块链上链数据结构和流程逻辑数据标准基础）：**



# 

# 应用场景分析及流程架构

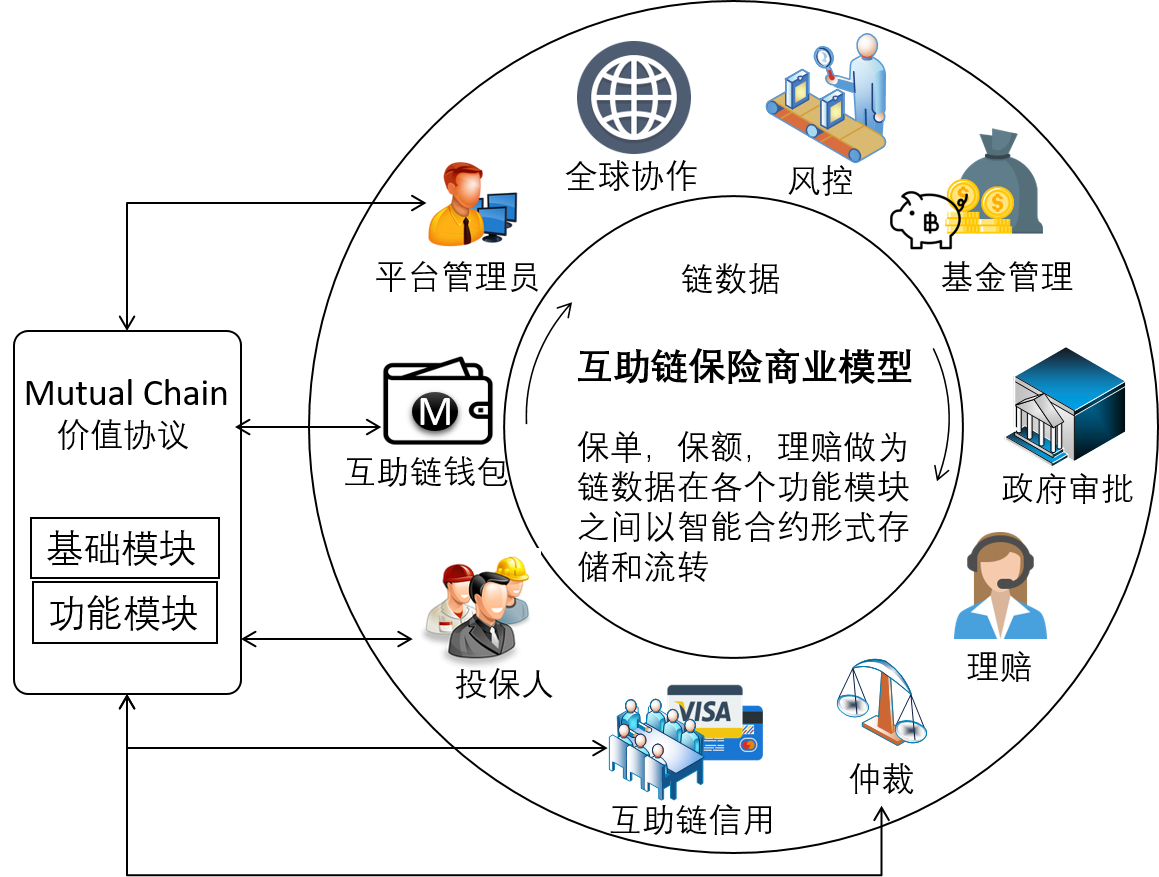
## 保险应用场景角色概述

互助链（Mutual Chain）的愿景是利用社会资本，信任网络和区块链技术来创建一个与所有参与者一致的保 险金融体系。大多数的草根阶层因为收入，工作环境和生活环境无法接触到保险产品可以带 来的保障和收益。这些未受到保险覆盖的民众在突发意外事件中是最无助的，而且也是受影响最大的。他们也在一直寻求可以替代的保险金融解决方案。我们相信今天的保险公司在社会中扮演着重要的角色。由于保险公司作为可以信任的第三方，即使他们提供无差异的保险产品，他们也可以获得丰厚的利润和蓬勃发展。我们相信对于可信任第三方有其他的替代方法，帮助减少集中式中介机构所带来的损耗，从而形成一个更具有包容性的普惠金融体系，到达人人可以获得基于公平的市场定价的保险产品。商业化保险追求利益最大化，特别是那些最需要的人，体现为运营成本高。政府提供的社会保险，医疗保险和失业保险对于草根阶层无法提供足够的保障。慈善帮助因为缺乏透明度而无法有效推广。其实这种金融基础架构已经在传统的社会中建立过，比如：互助会。互助会是有发起人的。发起人需要有足够的信用发起互助保险产品。我们的平台提供了对于发起人和互助会员零成本的接入。但是，发起人问题一直是互助保险的痛点，如何高效快速的让每个保单持有人参与投资决策，是区块链保险的一个优势，可以保证投资每个保单持有者有投票权。互助保险的发起人就相当于定义一个保险合约，包括合约的属性，内容和执行方式，参与者相当于加入并为这合约买单，通过区块链的方式共同执行。互助链前期可以主要解决已有的互助组织的问题，帮助他们更好的实现。互助链平台给用户一个定义不同属性合约的能力，并且通过绑定参与者和流通赋予这个合约。区块链在技术上通过共识建立了信用，传递价值。互助链就是实体社会的区块链，也是共识，信任和价值。

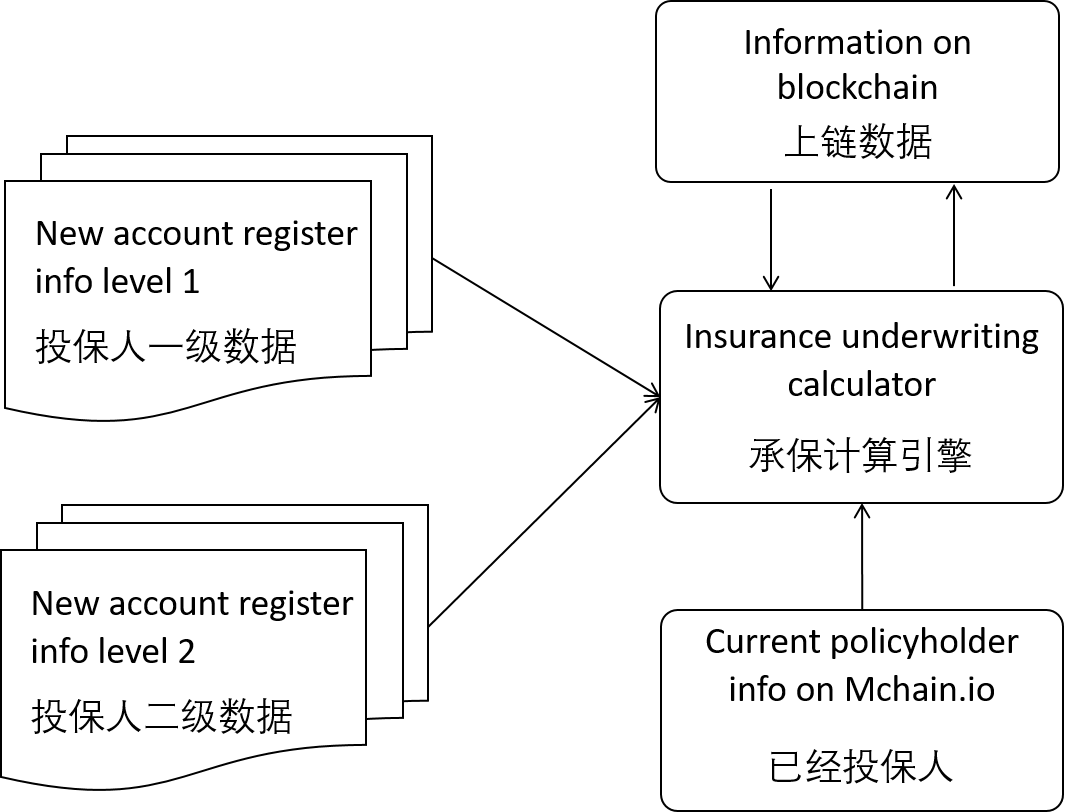
通过借鉴社区金融保险的凝合力和高效性，利用个人的信用和社会关系，我们可以重新互助保险形式。 当然，我们的产品和研究总是在进行中。 我们欢迎来自社区的意见，问题和想法并予以改进。互助链正在开发一个以社会资本，信托网络，区块链技术为动力的新型金融平台。同时我 们也会集成互助币的使用。这些代币具有加密货币的可交易品质，对于参与者广泛采用是至关重要的，而且它们可以与法定货币对应交换。互助链建立了一个分布的，可验证的信用身份。该身份根据遵守互助保险条款和联系社交媒体账户的品质而建立。负责任的个人将能够建立强大的信用身份，这将使其有更高的可信性，并最终具有提供更强大的社会效应，例如, 为其他成员提供担保的能力，并可以与社交圈外的人建立信任。 基于问责的集体行为效应远远大于个人行为效果。而且平台可以消除繁琐的官僚手续，减少欺诈，降低违约率。互助链通过基于数学研究，博弈理论，统计学和精算模型，以及计算模拟，将确保适当的激励措施符合所有各方利益。

互助链平台保险的执行方式，比如保险产品一旦绑定了参与方，智能合约会定期从参与方账户扣币，当参与方提出理赔申请，一旦满足预先定义的理赔条件，并所有参与方同意，机器逻辑自动从发起人扣币。如果是信贷合同的执行方式，包括贷款扣币，还款扣币以及利息扣币等等，这些都通过智能合约的执行和参与方验证交易，互助链在用户端就是建立一个可以发起和执行这些内容的工具。详细的流程，架构以及应用场景描述，请参考附录15.1.1

互助链还有其他若干应用场景，比如说商业和个人房地产贷款审批以及投资方案，详情可以参阅附录15.1.2



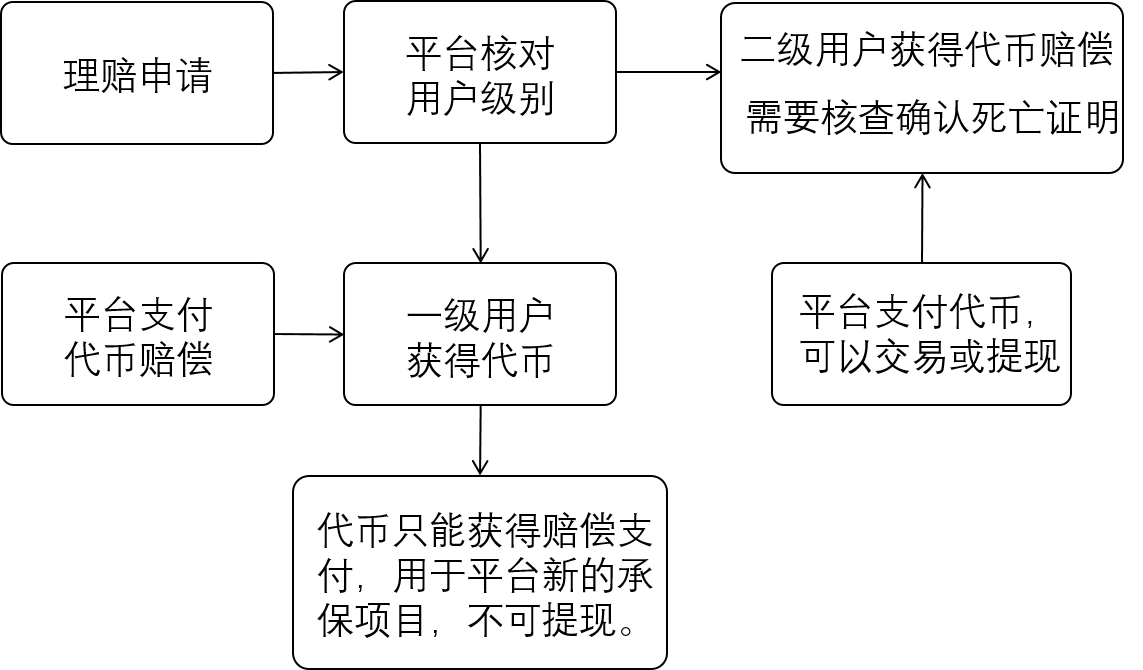
## 互助保险应用承保逻辑



1. Level 1 info only has: age, gender, e-wallet address, beneficiary’s age, gender and e-wallet address. Level 1 new account we only pays out coins and only allows the beneficiary to use coins to provide coverage to new accounts/new policyholders. We will not allow them to exchange coins to cash.
2. Level 2 info contains: ID, legal name, contact phone, wechat, QQ, bank account information, as well as beneficiary legal name, contact phone, ID. Etc. we will payout claim based on death certificate. With death certificate, we will allow beneficiary to exchange coins to cash in our platform.
3. Underwriting calculator needs information form new account info, existing info on chain and our own database in Mchain.io. please note, we only put very limited confidential information to blockchain, and we need to build our own 加密系统to send this information to chain.
4. Underwriting system is essentially an actuarial calculator for pricing.

## 互助保险应用理赔逻辑

1. 所有的理赔信息保存在平台中心服务器而不是放在互助链上；
2. 互助链保险平台MChain.io必须是唯一能决定哪些信息能上链的机构。



* All information on claims should be kept on Mchain.io, not blockchain.
* Mchain.io management is the only authority to decide which information will be shared on blockchain.

## 互助保险应用面临的问题和解决方案

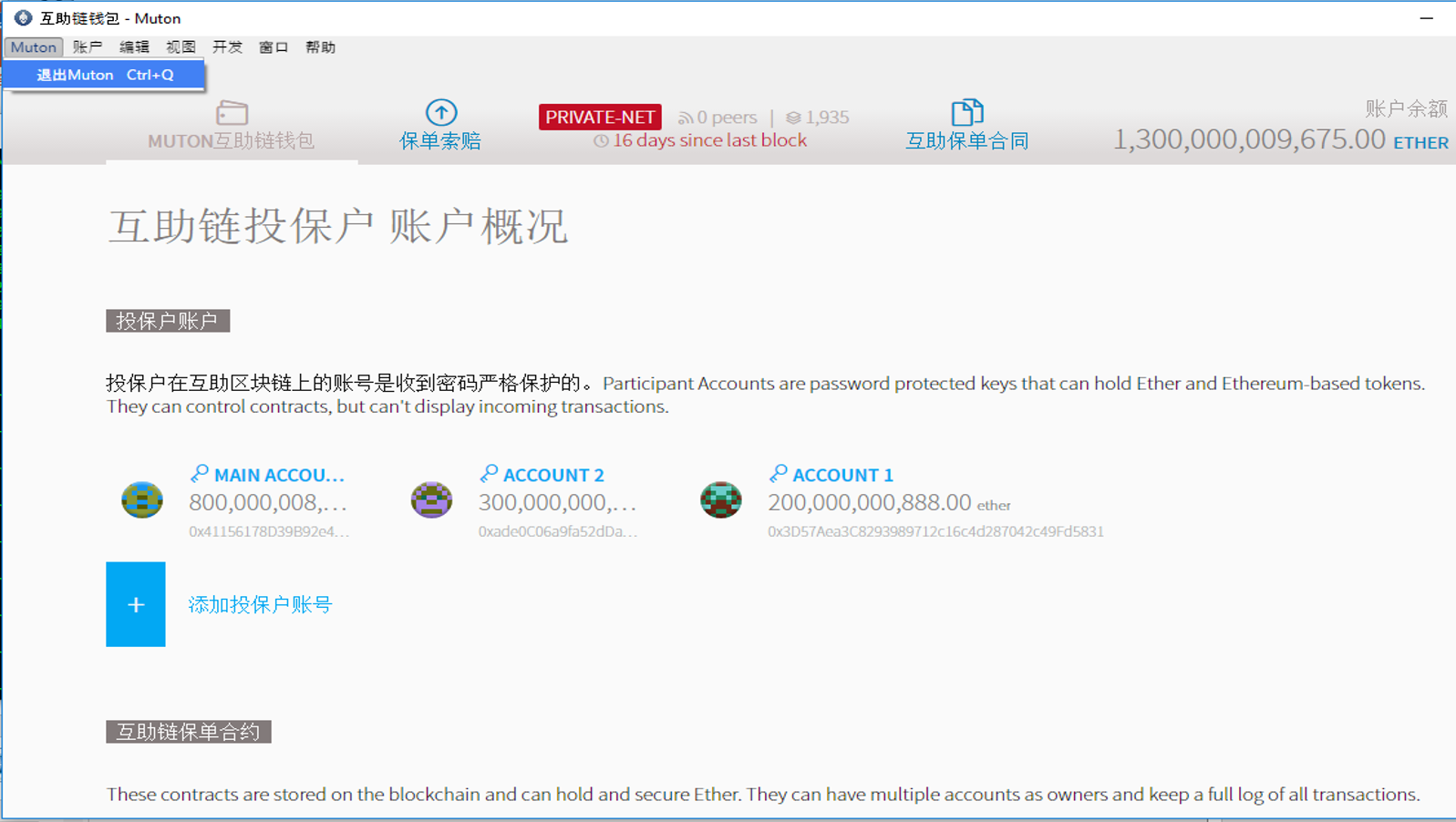
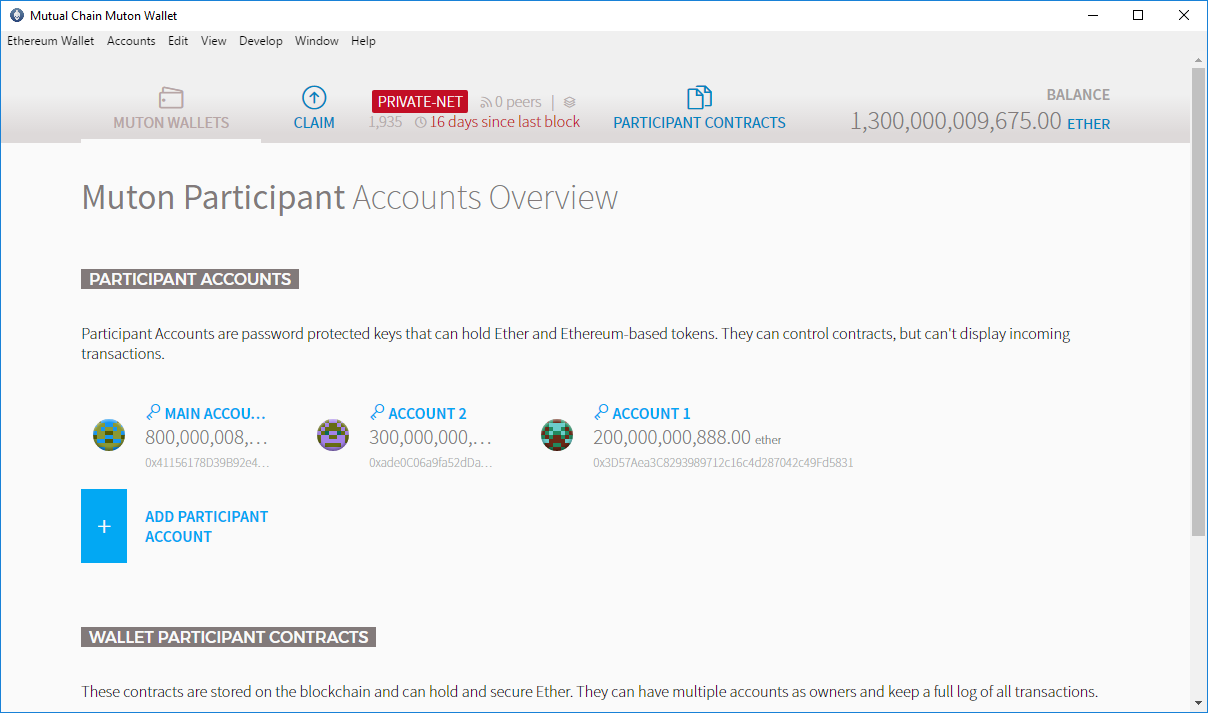
传统的保险缺乏有效的低成本的防欺诈机制。商业保险在签发保险前，通过严格的核保机制-派核保人员进行家访和全面的体检等手段尝试将潜在的风险控制在最低范围。在理赔发生时，调查人员亲自去到现场进行理赔调查和收集证据。这些都直接或间接导致非常高的经营开支。Mchain通过互助会的影响力和激励机制解决这个问题。

1. 信誉互评 – 互助会参加者将限制在可信赖会员范围内-家人，朋友，同事和社区组织成员。会员的失信行为会被记录，在亲友间失去信誉。这也符合互助会的理念，将互助会的规模和资金额度限制在适当的范围内来降低信用风险和确保会员间的诚信，会员互评也为之后的交易提供可靠依据。
2. 法律控制 – 通过电子签名的合同具有法律效力，会员之间相互绑定，确保彼此履行合约。会员需要为自己的违约行为承担法律责任。这种情况只有在会员个人风险高的情形下，司法程序才会具有意义。Mchain平台为会员创建自动填充合同的功能。
3. 产品设计 – 对于发起会员可以通过抵押来增加参与者的信心。抵押物将被纳入智能合约，如果违约或欺诈发生，抵押将会发放给遵守契约的会员。抵押可以是流动性高的数字资产如比特币等，也可以是固定资产如汽车，房产。抵押可以提高资本的利用效率。对于新加入的，信誉还没有建立起来的会员，只可以参与风险低的保障条款。随着会员的信誉提升，该会员会享受更多的保障。
4. 激励机制 – 假如会员违约，为了追回资产，互助会将发起奖励金。奖励金会在追回后付给帮助追回的会员。

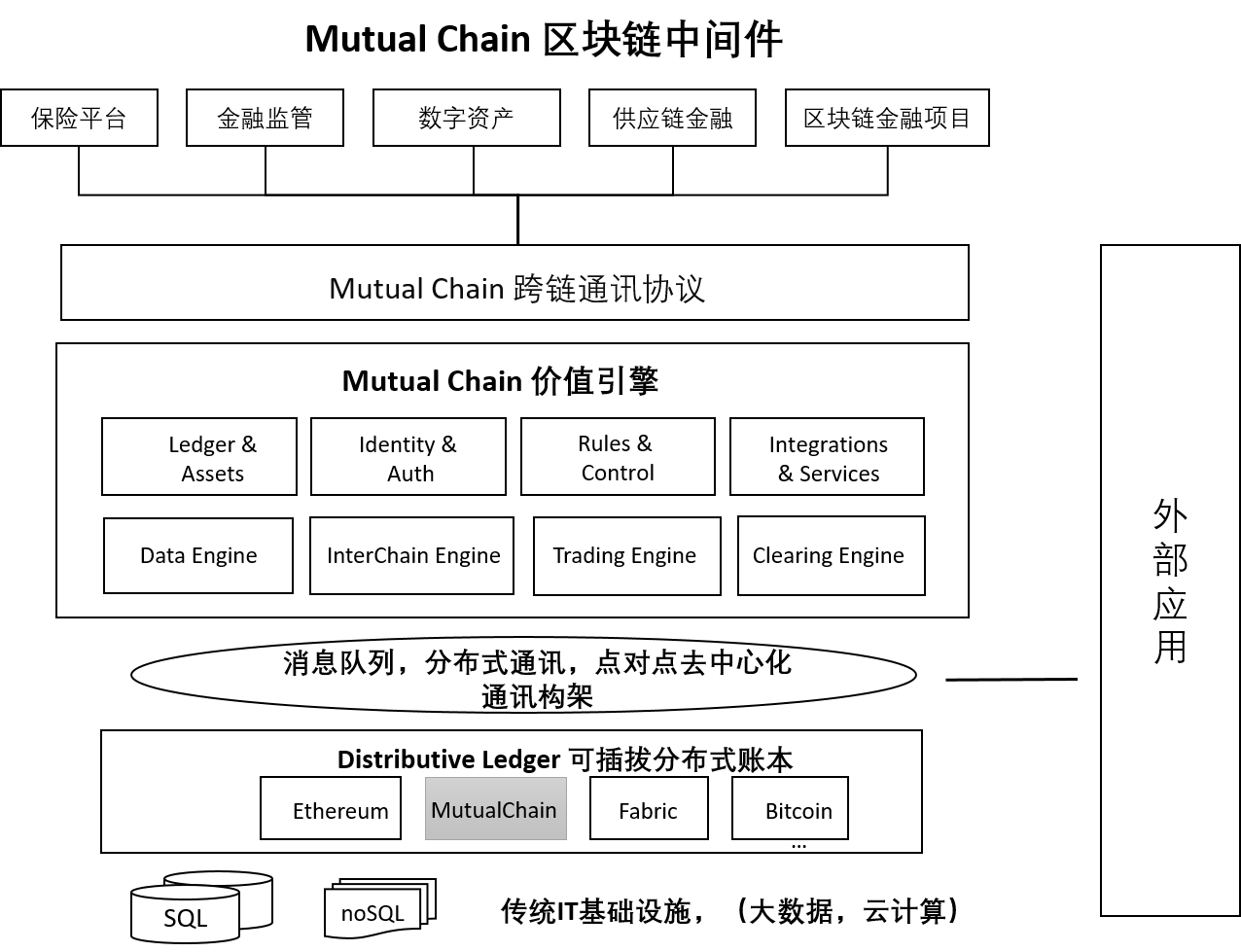
这些预防机制是基于自愿原则，会员可以自行设定其安全性，这些在实际运用时都比较灵活，可以根据资助会特性相应的修改。

传统的互助会很难大规模的扩张。通常来讲，会员必须处于共同的社区圈子，以便参与决议和亲自管理。因此大型的互助会难以成型，同时也限制同一会员同时参加多个互助会。Mchain致力于利用区块链和移动技术解决互助会现有的不足，特别是针对中国等发展中国家的中产阶级用户。区块链促进互助会透明化。所有关于互助会的重要信息将安全准确地在区块链上自动存档。这些档案将对所有会员公开。区块链去除第三方管理的必要。区块链技术实现自动付款和归档。用户因此可以自行管理互助会，无需外界介入。一个成功的互助会建立了成员之间的信任。该互助会的信誉可以吸引其他人员加入互助会。并且其他地域的互助会可以参照成功模式进行复制，从而克服了传统互助会所面临的问题。

# 互助链区块链浏览器与钱包



# 互助链区块链中间件构架



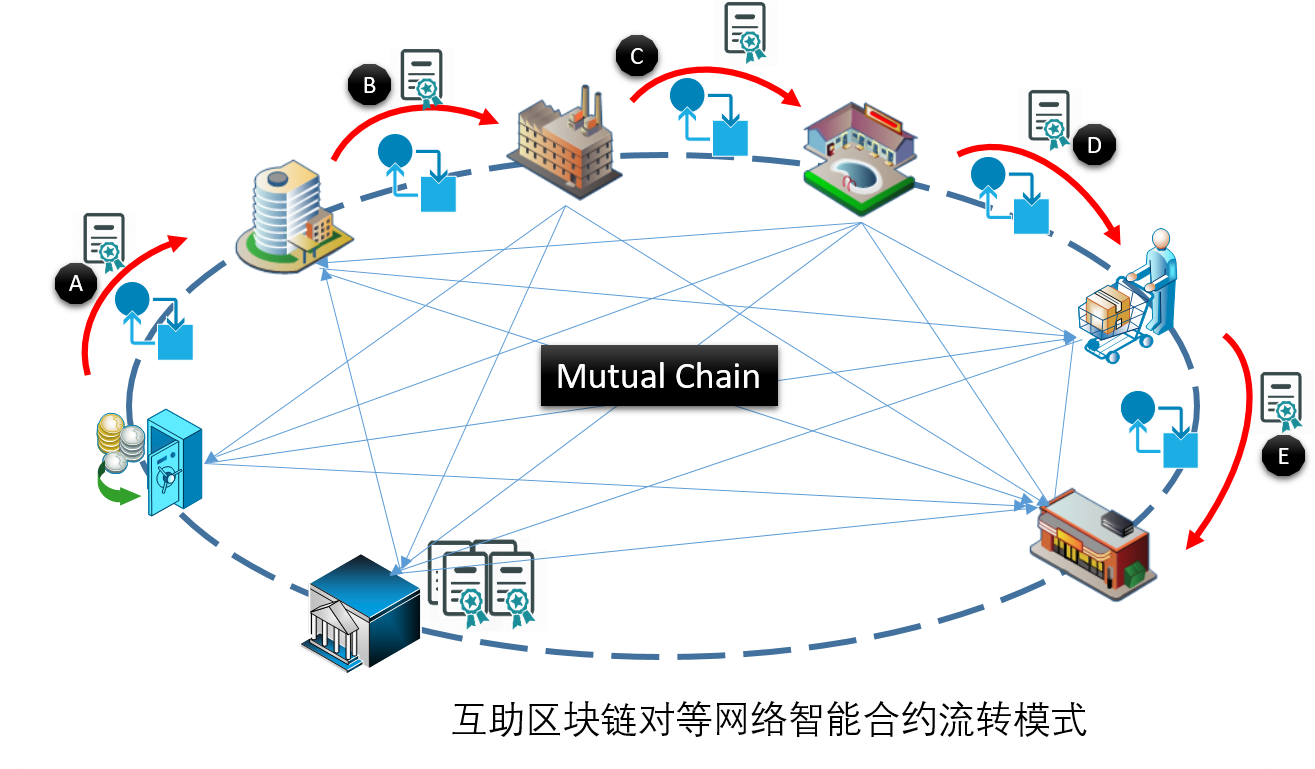
## 互助链跨链价值网关

**互助链跨链价值网关** - 是一个可以跟多个不同技术架构的异构价值网络进行通讯并能将资产数据进行自由转换的，可扩展，开放的软件接口。

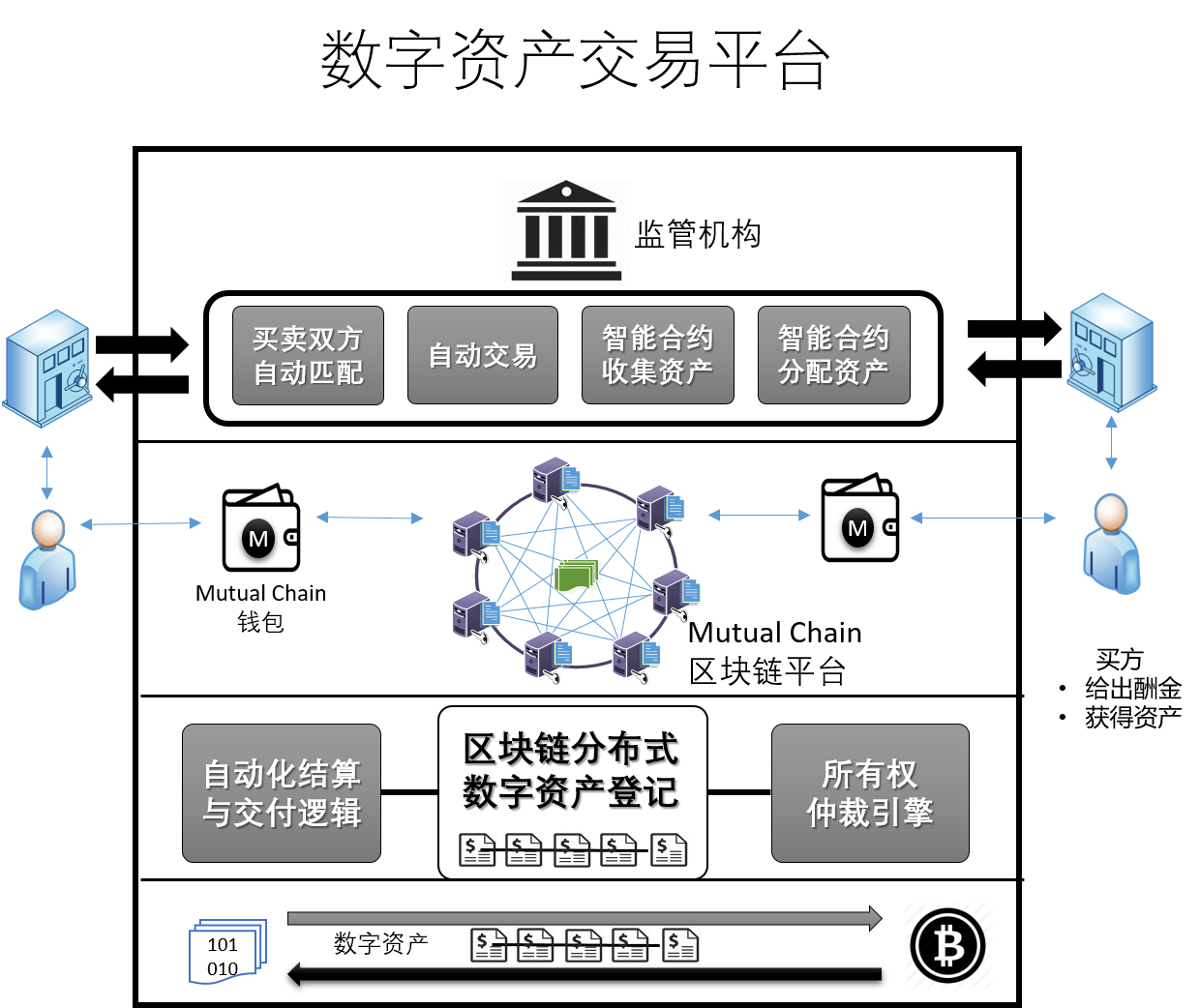
## 互助链Fintech引擎

**互助链金融科技引擎**- 包括未来可能的区块链数据读写交换引擎，资产交易，供应链金融逻辑，资产结算和清算引擎等。

# 互助链智能合约逻辑



# 互助链数字资产与交易



* 分布式交易账本
  + 第一次将资产完全数字化
* 数据更安全更具公信力
  + 完全透明公开的交易数据和交易历史，不可篡改，任何人（包括交易所平台的监管和运营）都不可以挑战数据的
* 交易根据智能合约自动匹配，更公平公正高效
* 交易资产上链存证，产权和所有权管理更方便
* 结算清算交割自动化与智能合约化，降低交付成本甚至消除大量繁琐的交易前中后台工作
* 消除交易双方对手风控
* 担保保险融资和政府监管更透明高效

# 互助保险系统

## 为什么选择以太坊

也许出于安全性的考虑，比特币所提供的脚本语言并不是图灵完备的，能力有限，并不能完成现实世界里的大多数计算问题。同时比特币网络本质上是一个状态的转移系统，在比特币系统里，有一个包含现在所有已存在的比特币的持有者的状态，并且有一个“状态转移函数”可以使用一个状态和一个交易来产生一个新的状态。且比特币系统只有UTXO概念，对某个地址的查询效率低下。以太坊的概念是在2013至2014年间由Vitalik Buterin提出，其目的是研发出 “下一代加密货币与去中心化应用平台”，并在2014年通过ICO而得以开始发展。实现整个以太坊系统的是开源代码，其核心是基于专有加密货币的以太币（Ether）的公共区块链平台。在这个平台之上，以太坊提供了去中心化的以太坊虚拟机，方便其他第三方研发人员来实现基于以太坊的智能合约。以太坊虚拟机使得第三方研发人员能够简单快捷地重复利用以太坊所定义的区快链核心系统，同时能够把自身的研发重心放在区块链的应用上。

相较于大多数其他区块链技术，以太坊平台提供能账户，虚拟机和智能合约。大大提高了开发DApp的效率。

## 智能合约平台

支持智能合约体系的关键部分是以太坊虚拟机（Ethereum Virtual Machine ），它提供了一套类似汇编语言的图灵完备语言，可以执行任意复杂算法的编码，用来桥接数据处理和应用处理。互助链是类似于以太坊的区块链结构，用户的担保，承保，赔付，收益都以智能合约的形式写入底层区块链中。这样做的好处在于：

* 去除中间环节，降低成本
* 合约强制执行，不需要人工干预
* 资金的使用，流向公开，透明

以太坊上要写智能合约有好几种语言可选：有点类似Javascript的Solidity, 文件扩展名是.sol. 和Python接近的Serpent, 文件名以.se结尾。还有类似Lisp的LLL。我们为互助链选择了Solidity。DApps的打包工具我们选择Truffle。基于以太坊虚拟机以及Solidity编程语言，我们就可以开发出以太坊智能合约。简单来说，每一个合约都是一个基于以太坊区块链系统的分布式应用程序。当研发人员将一个开发出的合约在以太坊平台上上线后，这个合约就类似于一个活在以太坊平台里的应用代理人，它拥有自己的以太币地址，可以用来进行以太币交易、可以和创建者以及其他使用者交互信息、也可以用来执行具有复杂逻辑性的应用，譬如建立一套基于以太坊的代币系统、发起一次ICO活动以及建立一个去中心化自治组等等

## 系统框架

由于区块链具有完全公开、高可靠性、即时交割、去信任等诸多优点，我们设计了一个基于区块链的互助保险系统。它主要由4层架构：网页/移动客户端，基于区块链的业务逻辑管理模块以及数据存储模块。

**移动端**

**Web 端**

**客户端**

**业务端**

**AI**

**身份认证**

**资金池管理**

**精算**

**智能合约n**

**区块链**

**智能合约1**

**智能合约k**

**担保数据库**

**数据端**

**承保数据库**

**保险合同**

## 互助币

互助币是基于以太坊ERC20协议开发出的代币，这样可以使得互助币在ICO结束后很方便地上线全球重要数字货币交易平台。同时也支持转账和查询余额**。**互助币被用来构建保险系统的资金池，用户可以充值兑换成互助币，利用互助币来支付保险费用，各种手续费用或者赔付费用。在用户选择离开互助保险平台时，用户可以提取与其互助币价值相当的真实货币。随着互助保险生态的丰富，互助币应该会承担越来越丰富的角色：互助币不仅能支付，理赔，而且应该能在重要的数字货币平台上和其他数字货币进行交易，具有投资属性。互助币是信用传递到价值的转换。比特币就是从一群极客的社区信用变为目前的社会认可价值。另外，互助币也会在ICO和众筹中扮演重要角色。

## 人工智能模块

传统的保险行业沿用的是工业时代的规则，先圈定目标人群，然后为不同的目标人群设计不同的保险品种，注重规模化效应，所有投保人都被置于同一风险水平之上，而完全忽视了人群中的个性化差异。进入互联网时代以后，个性化差异问题越来越突出。功能的定制化和精准营销成为潮流。保险行业也从名目繁多的保险种类，发展到针对个人需求定制保险以及自主发现新的保险种类。以前，由于计算机技术手段的限制，扑捉个性化差异并推出相应的保险产品，人类有些力不从心。而随着大数据时代的到来以及计算机算力的提高，近年来人工智能取得了极大的突破。这就为保险行业的颠覆性改变提供了契机。

互助保险系统的人工智能模块通过运用人工智能最新的研究成果，实现精确的风控模型和定价策略，通过对个体的基于大数据的智能分析，实现：

* 个性化保险设计
* 精准化推销
* 自主发现新的保险品种
* 精确地理赔

## 风险防范

2017年7月20号的以太坊钱包漏洞让以太币价格大跌，让数字货币持有人心惊胆颤，也让投资人的信心动摇。但是正如Vitalik Buterin针对此次漏洞的回应，这次事件不是以太坊的漏洞，它只是一个编码漏洞而已，所以也不需要硬分叉。此次事件是由于智能合约编程那个语言Solidity的问题。在互助币的发行和运营过程中，我们可以采用以下措施，提高安全性，以保护用户的投资以及互助保险系统的平稳运行：

* 由于互助币是建立在联盟链的基础上，我们可以将智能合约的代码不公开。仅仅对于经过资格审核的伙伴公开
* 互相做严格的代码审查
* 采用安全的开发流程

单元测试

私有链测试

测试链测试

* 功能解耦

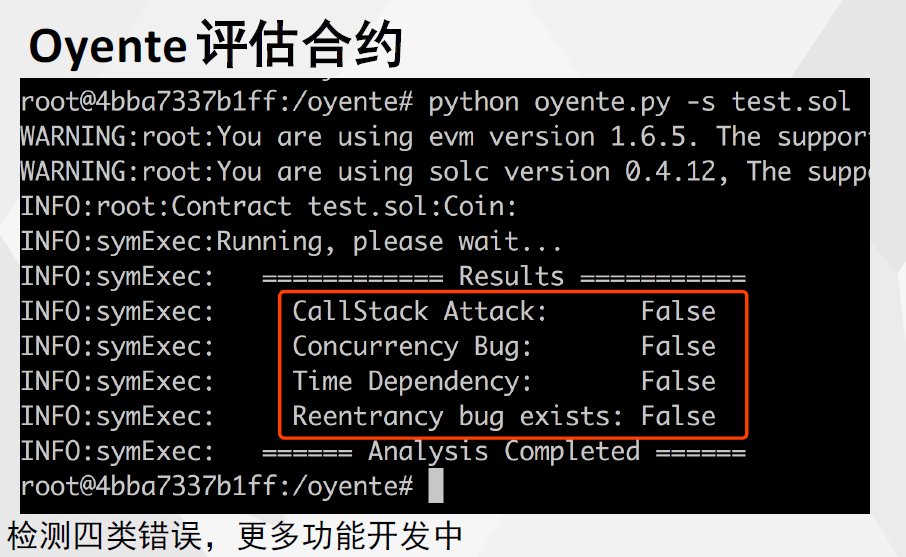
正交分解

逻辑简单

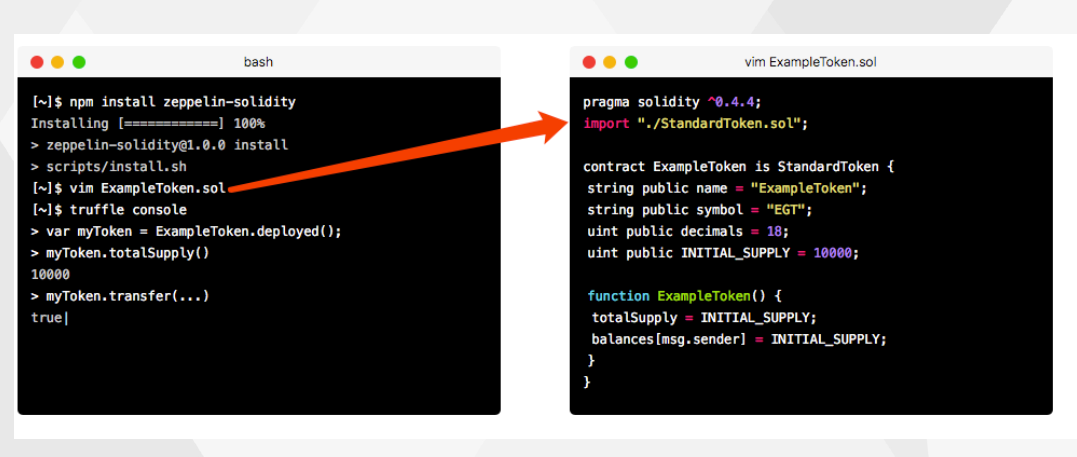
只对最核心的部分去中心化

* 安全相关的工具

Oyente



Zeppelin



Zeppeline提供了更安全的组件：

* + 安全数值运算，防止溢出
  + 所有权管理
  + 支付，余额以及限制每日交易数量
  + 多重签名
  + Token抽象类和安全实践

# 互助链应用实例：一个互助保险的说明

小明是非常典型的数字货币早期投资人：

1. 入市早，持有一定的比特币
2. 长期持有，对比特币的升值抱有乐观积极的看法
3. 讲究生活品质，愿意尝试新的事物
4. 注重自己和家人的财务规划，希望提前规划和规避重大风险，尤其是人身风险

然而，目前市场上没有太多金融产品的选择：

1. 传统的保险公司销售的人寿保险产品，无法满足小明对数字资产增值的需求；
2. 新兴的数字货币市场，没有成熟的保险产品满足小明的需求，甚至，没有一个公司或者一个组织能够提供简单的产品

在比特币投资的圈子中，小明发现了mchain.io,一家为数字货币圈的小伙伴们提供数字资产为基础的人寿保险的平台。小明对这个平台产生了兴趣。

小明来到mchain.io,他发现可以以两种身份来注册：一种是自己现实世界中真实的身份，既身份证定义的身份；一种是数字身份，既通过区块链的数字信息定义的身份。Mchain.io提供的人寿保险，可以连接两个身份，也可以把两个身份完全分开。不同的是，真实身份的小明，很大概率活不过120岁，而数字身份理论上而言，只要区块链存在，是永不熄灭的生命。

小明把两个身份都注册了，并且没有把两个身份关联。理论上而言，小明可以拥有无限的数字身份，只要他的比特币足够多。

完成身份信息提交后，小明选择用真实身份在mchain.io上，通过连接自己的银行账户，购买了一个比特币，用于在平台上来购买人寿保险。

同时，小明用数字身份，通过自己的比特币电子钱包，为自己在mchain.io的账户中转入了一个比特币，用来购买平台上的人寿保险。

平台的人寿保险账户被激活的最低要求是，在账户中至少有一个比特币。

小明在比较了平台提供的人寿保险后，决定在1年期，2年期，5年期，和终身保险中，选择终身保险。选择这一产品的主要原因是，前三个保险产品是纯粹的保险，而终身保险，可以通过互助保险的资产收益账户，享受到为其他新加入的互助保险成员提供保险的保费收益。

小明仔细的看了平台细则后，发现保险的赔付部分是如下运行的：

保险的保费是一个比特币，需要存入mchain.io的信托账户。如果真实身份的小明过世，而过世年纪是在0到55岁，那么保险会赔付10个比特币，如果是在56岁到85岁之间过世，那么保险赔付5个比特币，如果是在86岁到100岁之间过世，保险赔付2个比特币。在100岁时，不论小明是否过世，平台都会把这一个比特币还给小明，既退还到小明的mchain.io账户。小明的保险受益人，或者小明本人，都可以在平台用比特币兑换成法币，然后转到银行账户。

小明的数字身份无法确定年纪，虽然小明选择的也是终身保险，然而保费的支付方式确不同。除了在一开始，小明需要把一个比特币转入mchain.io的信托账户，小明还需要每隔360天（近似一年），就向mchain.io的账户打入0.01个比特币。当连续5次没有新的比特币打入账户后，mchain.io判断小明的数字身份为过世。保费的赔付额度取决于连续多少次打入保费。表格如下：

|  |  |
| --- | --- |
| N = 连续打入保费的次数 | 赔付额度 |
| 0-55 | 10 + N x 0.01 |
| 56-85 | 5 + N x 0.01 |
| 85-100 | 2 + N x 0.01 |
| >=100 | 1+ N x 0.01 |

除了赔付，小明也仔细看了资产收益账户的运行模式。

真实身份和数字身份的资产收益账户运行都是相同的。当小明加入互助保险的时候，平台已经有20万成员，而且和他非常像，都是数字货币圈子里的朋友，虽然，他们之间并不知道对方是谁。

初始时，平台的信托中已经有至少20万枚比特币。信托的保守投资策略竟然在目前的市场也可以保持40%的年回报率。Mchain.io会收取相应的投资管理费用。

同时，每当有一个数字身份加入互助保险平台，每个现有的成员，在资产收益账户中，会有相应的一笔保费收入。当然，当某一个投保人过世的时候, mchain.io 的链和平台会同时更新信息，而且自动从资产账户中扣除需要的赔付部分。

由于数字身份的特殊性，只要一直付保费，就可以一直享受资产收益，而且超越100岁的限制。

当投保人过世，或者被判定过时的时候，资产账户的收益，自动转入mchain.io上小明的账户，或者小明选定的受益人账户。

# 互助链Muton币ICO及ICO之后的项目情况

## 互助币Muton（代币符号:MUC）的发售

## 互助币的锁定机制

## 互助币最低筹集资金和资金使用情况

# 互助链开发计划与预算

# 互助链团队

（见附件）

# 附录

## 其他应用场景详述

### 互助链架构应用于保险流程的优化

Blockchain’s value for Insurance

External Reporting

Claims

Post Bind

Accounting & Settlement

Placing

## 

***Blockchain has the potential to drive simplicity and efficiency through the establishment of new financial services infrastructure and processes across all of the key aspects of the insurance value chain***.

Operational simplification: Reduces manual efforts to reconcile and resolve disputes;

Counterparty risk reduction: Agreements codified and executed in a shared, immutable environment;

Liquidity and capital improvement: Can reduce locked-in capital and provides increased transparency;

Regulatory efficiency improvement: Enables real-time monitoring;

Clearing and settlement time reduction: May reduce some third parties supporting transaction verification / validation and accelerates settlement;

Fraud minimization: Helps with asset provenance and transaction history within a single source;

**Insurance Administration:**

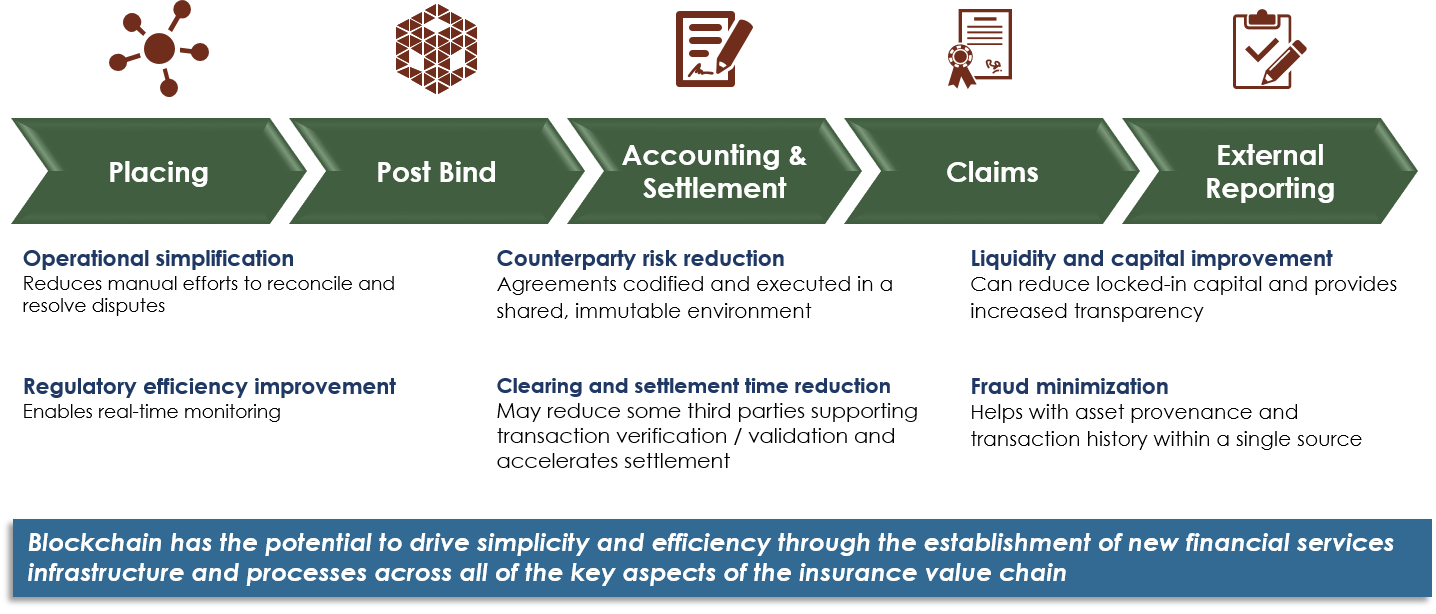
Today:

1. Manual processes between multiple parties (Insurance provider, benefits administrator, employer, employee, service provider network, etc)
2. Protracted coordination of business transactions between business network participants
3. Different versions of the same data in multiple systems of record, leading to added costs and lengthy disputes
4. Error prone verification processes for eligibility and benefits

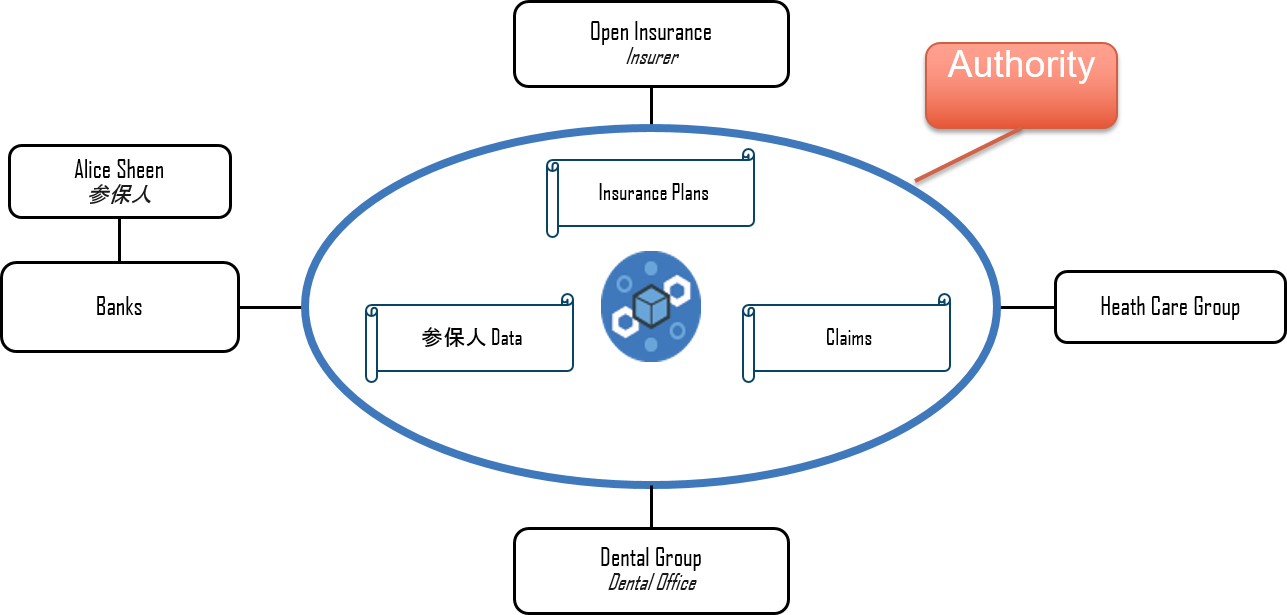
With Blockchain:

1. Manual process are automated by sharing plan participant, entitlement and claim data
2. Smart contracts computationally encode participant registration and verification rules
3. Shared data and smart contract computations reduce downstream disputes
4. Benefits verification based on multiple data sources readily available to all service providers

#### Blockchain’s Value for Insurance



#### Blockchain Network Participants



#### 应用场景一（互助保险）

Client registers on mutual insurance exchange and create own wallet

* verify personal information
* link bank account to exchange
* setup private key and wallet for policyholder and beneficiary
* System maintenance cost and Blockchain gas
* Investments and reinsurance

Client buys ETH or BTC coins from exchange

* Exchange prepares quote based on client request on coverage
* Smart Contract is initialized between each policyholders to mutually cover each other

Client shops on life insurance coverage on exchange and quote premium in mutual insurance coin

Client buys mutual insurance coin (smart contract) to engage with current mutual insurance policyholders

* Smart contract distributes new coverage coins equally to each current policyholders
* Each current policyholder gets new coverage coins portion and agrees to lock it until coverage expires or payout as part of death claims

Blockchain broadcast event

Smart contract executes based on survivorship certificate and expires coverage between policyholders and unlock mutual insurance coverage

Smart contract executes based on death certificate and mutual policyholders pays mutual insurance coin to beneficiary wallet

Plan Participant Onboarding (Insurance Sales): Interactions between Plan Sponsor and Plan Administrator to on-board Plan Participants is often cumbersome and error prone

Role of Blockchain:

* Records required plan participant information directly from Plan Sponsor’s HR systems
* Makes data available to all blockchain participants on a real-time basis reduces possibility of dispute
* Improves client satisfaction and reduces costs

#### 应用场景3

Coverage Verification:

Lack of ready availability can:

- Delay provision of coverage upfront

- Involve cumbersome manual discussions

- Require upfront payment despite coverage

Role of Blockchain:

* Provides immediate access to coverage information and current plan participant status
* Smart contracts verify plan participant coverage immediately, and avoid creation of payment disputes after the appointment occurs

#### 应用场景4

Claim Submission:

Initial submission and filing process can:

- Allow erroneous submissions

- Result in dispute resolution

- Delay payment times

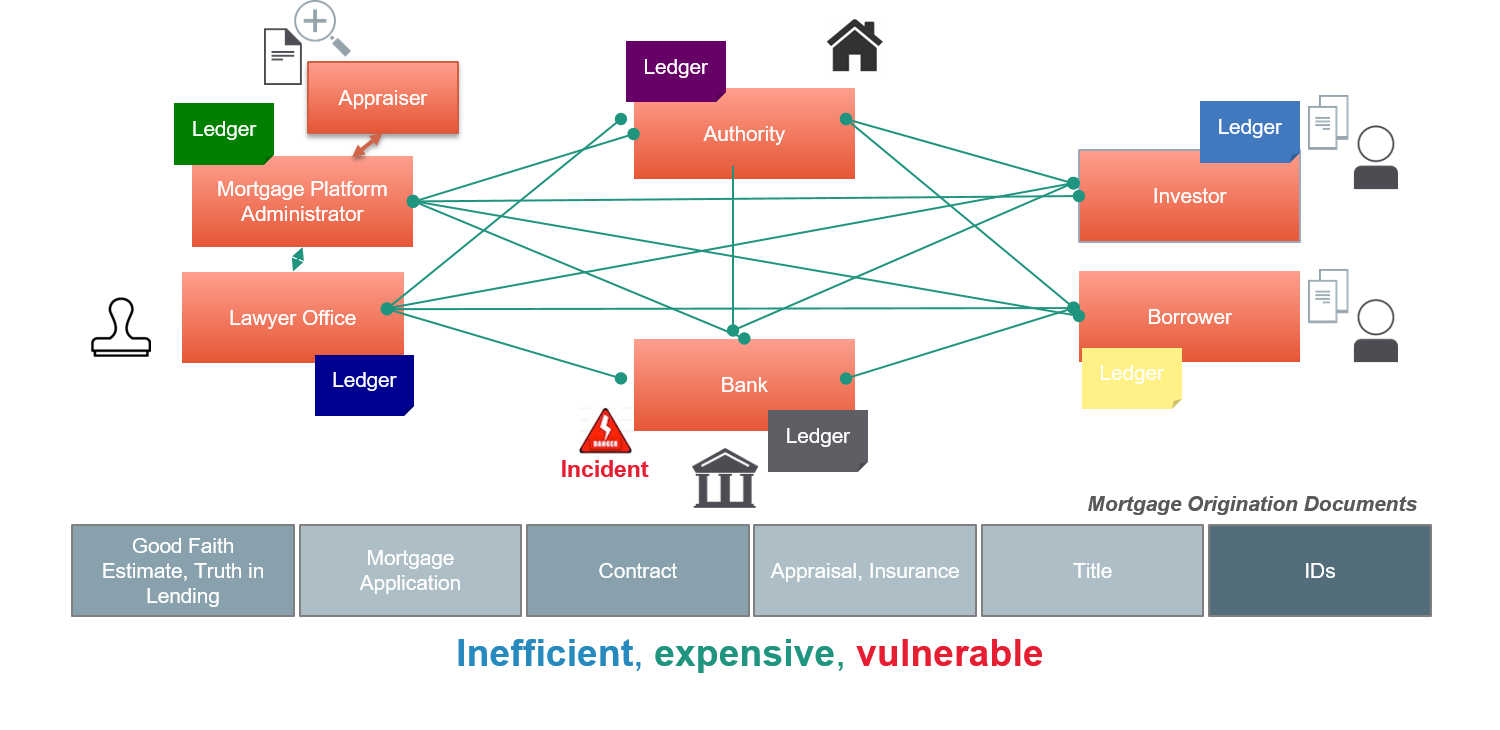
Role of Blockchain:

* Provides smart contracts that capture key contractual elements of the underlying policy and flag claim errors before submission
* Gives all permissioned parties access to claim data
* Provides immediate access to more relevant data and reduces the time required to make business decisions

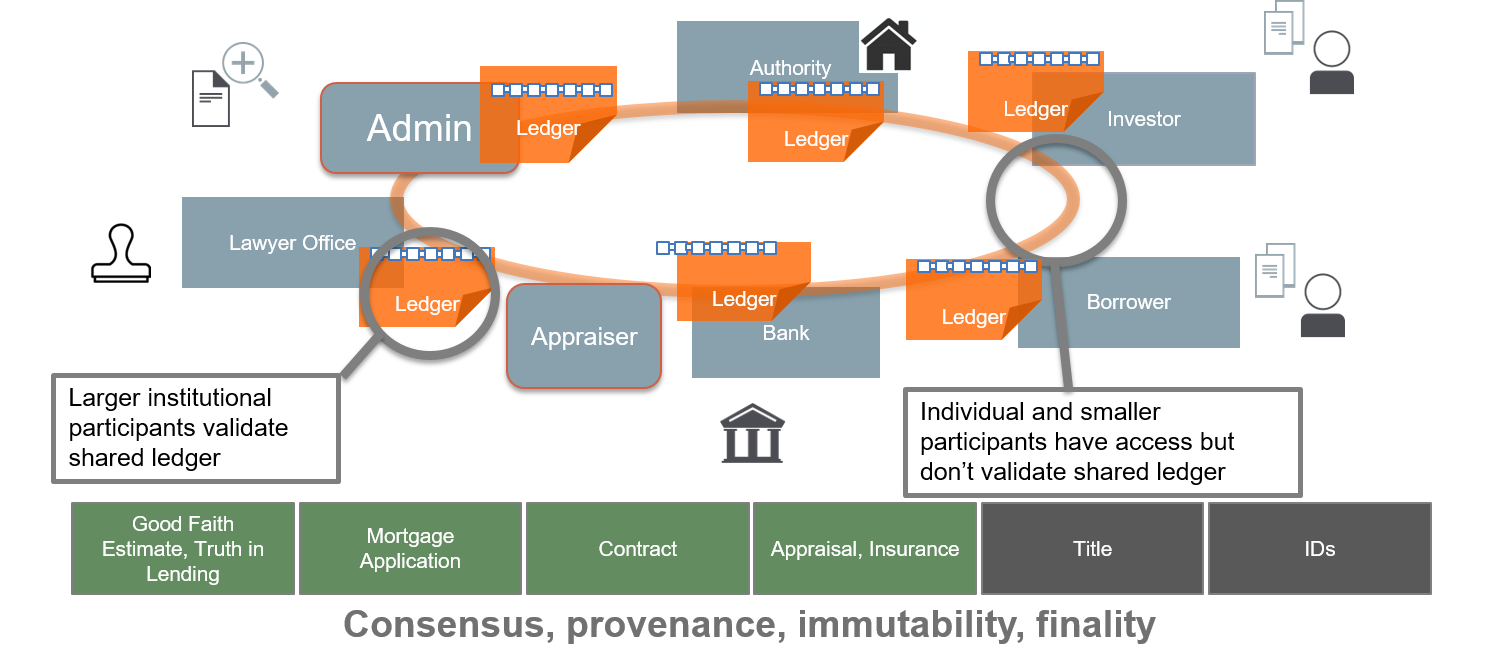
### 互助链架构应用于房屋贷款审批及投资平台

#### Mutual Chain Mortgage Origination: Processes are timely, costly and can result in search errors, which generate transactional risk

# 



#### Mutual Chain A shared ledger between involved parties can increase trust, speed of execution, auditability and cost



## 项目组织结构

### 核心团队

第一阶段，我们预计需要建立7-11人的国际团队，具体包括：

* 项目总监委员会
* 执行总监(1)
* 区块链技术主管/架构师 (1~2)
* 区块链研发工程师 (3~5)
* 前端开发设计 (1)
* 保险逻辑和产品开发 (1~3)

### 角色与责任

|  |  |  |  |
| --- | --- | --- | --- |
| **团队** | **角色** | **姓名** | **负责的具体工作** |
| 项目总监委员会 | 委员会成员 |  |  |
| 执行与运营 | 执行总监 |  |  |
| 架构师 | 区块链架构师 |  |  |
| 区块链技术主管 |  |  |  |
| 区块链研发工程师 |  |  |  |
| 前端开发设计 |  |  |  |
| 保险逻辑和产品开发 |  |  |  |

## 主要里程碑Key Milestone

|  |  |  |
| --- | --- | --- |
| **#** | **里程碑** | **日期** |
|  | Phrase I |  |
|  | Phrase II |  |

**参考文献**

|  |  |
| --- | --- |
| [1] | Satoshi. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: <http://bitcoin.org/bitcoin.pdf>. [Accessed 10 09 2015]. |
| [2] | Vitelik. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform”, 2013. <https://github.com/ethereum/wiki/wiki/White-Paper> |
| [3] | Gavin. Wood, "Ethereum: A Secure Decentralized Generalised Transaction Ledger," 2014. <http://gavwood.com/paper.pdf> |
| [4] | ERC 20 Type Tokens. “ERC: Token Standard” q  <https://github.com/ethereum/EIPs/issues/20> |
| [5] | David. A. Johnston, “The General Theory of Decentralized Applications, Dapps”, 2014. <https://github.com/DavidJohnstonCEO/DecentralizedApplications> |