

OATH

# OATH 众裁协议

区块链链上治理纠纷化解协议

Yin Xu  
Oaths.io  
Version 2.4.0

## **DISCLAIMER -- READ BEFORE CONTINUING**

This white paper is for information purposes only and may be subject to change. This white paper does not constitute an offer or solicitation to sell securities. Any such offer or solicitation will be made only by means that are in compliance with applicable securities and other laws. No information or opinions presented herein are intended to form the basis for any purchase or investment decision, and no specific recommendations are intended. Accordingly, this white paper does not constitute investment advice or counsel or a solicitation for investment in any security. This white paper does not constitute or form part of, and should not be construed as, any offer for sale or subscription of, or any invitation to offer to buy or subscribe for, any securities, nor should it or any part of it form the basis of, or be relied on in any connection with, any contract or commitment whatsoever. Oath Holding Ltd., a British Virgin Islands business [Company] ("OATH") [and its affiliates (collectively, the "Company")] expressly disclaim any and all responsibility for any direct or consequential loss or damage of any kind whatsoever arising directly or indirectly from: (a) reliance on any information contained in this white paper; (b) any error, omission or inaccuracy in any such information; and (c) any action resulting therefrom.

[The Company] cannot guarantee the accuracy of the statements made or conclusions reached in this white paper. [The Company] does not make, and expressly disclaims, all representations and warranties (whether express or implied by statute or otherwise). This white paper does not constitute advice, nor a recommendation, by the Company, its officers, directors, managers, employees, agents, advisors, or consultants, or any other person to any recipient of this white paper. This white paper may contain references to third-party data and industry publications. As far as [the Company] is aware, the information reproduced in this white paper is materially accurate and such estimates and assumptions therein are reasonable. However, there are no assurances as to the accuracy or completeness of such reproduced information. Although information and data reproduced in this white paper is believed to have been obtained from reliable sources, [the Company] did not independently verify any of the information or data from third party sources referred to in this white paper or the underlying assumptions relied upon by such sources.

[The Company] makes no promises of future performance or value with respect to its proposed business operations, Simple Agreements for Future Tokens ("SAFTs") or OATH (as defined herein), including no promises of inherent value, no promises of payments, and no guarantees that SAFTs or OATH will hold any particular value. Unless prospective participants fully understand, comprehend, and accept the nature of [the Company]'s proposed business and the potential risks inherent in SAFTs and OATH, they should not participate in [the Company]'s sale of SAFTs or any OATH.

The offer and sale of the SAFTS and any OATH have not been registered or qualified under the securities, investment or similar laws of any jurisdiction anywhere in the world, including under the United States Securities Act of 1933, as amended (the "Securities Act"), or under the securities laws of any U.S. state. The SAFTs and any OATH are being offered and sold solely outside of the United States to non-U.S. Persons (as

defined in Regulation S under the Securities Act ("Regulation S")) ("U.S. Persons") and only in jurisdictions where such registration or qualification is not required, including pursuant to applicable exemptions that generally limit the purchasers who are eligible to purchase the SAFTs or any OATH and that restrict their transfer or resale. The offer and sale of the SAFTs or any OATH does not constitute a public offer of "investments" or "securities" in the British Virgin Islands. The purchaser is required to inform itself about, and to observe any restrictions relating to, the SAFTs and any OATH and any related documents in the purchaser's jurisdiction. The SAFTs may not be offered or sold in the United States or to or for the benefit of U.S. Persons unless they are registered under the Securities Act or an exemption from the registration requirements of the Securities Act is available. Hedging transactions involving the SAFTs may not be conducted except in compliance with the Securities Act. The SAFTs and any OATH may not be offered, sold or otherwise transferred, pledged or hypothecated except as permitted under applicable law.

No regulatory authority has examined or approved any information set forth in this white paper. No such action has been or will be taken under the laws, regulatory requirements, or rules of any jurisdiction. The publication, distribution, or dissemination of this white paper does not imply that applicable laws, regulatory requirements, or rules have been complied with. SAFTs and OATH may be impacted by regulatory action, including potential restrictions on the ownership, use, or possession of OATH. Regulators or other authorities may demand that [the Company] revise the mechanics and functionality of OATH and [the Company]'s proposed operating model to comply with regulatory requirements or other governmental or business obligations.

The distribution or dissemination of this white paper or any part thereof may be prohibited or restricted by the laws, regulatory requirements, and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this white paper or such part thereof (as the case may be) at your own expense and without any liability to the Company. Persons to whom a copy of this white paper has been distributed or disseminated, provided access to, or who otherwise have this white paper in their possession shall not circulate it to any other persons, reproduce, or otherwise distribute this white paper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

## **CAUTION REGARDING FORWARD-LOOKING STATEMENTS**

Certain statements in this white paper constitute "forward-looking information" under applicable securities laws. Except for statements of historical fact, information contained herein constitutes forward-looking statements, including (i) the projected performance of the Company; (ii) the completion of, and the use of proceeds from, the sale of the SAFTs; (iii) the expected development of the project; (iv) the execution of vision and growth strategy, including with respect to the OATH's future global growth; (v) the sources and availability of third-party financing for the project; (vi) the completion of the project currently underway, in development or otherwise under consideration; (vii) the ability to launch a functional platform, which is related to the creation and issuance of OATH and the associated economic value thereof; and (viii) the future liquidity, working capital, and capital requirements. Forward looking statements can also be identified by words such as "can," "expected," "will" and other identifiers of non-historical events. Forward-looking statements are provided to allow potential purchasers of the SAFTs the opportunity to understand management's beliefs and opinions in respect of the future. [the Company] is at an early stage [Company] with a product in development, and an investment in SAFTs is inherently risky.

These statements are not guarantees of future performance, and undue reliance should not be placed on them. Such forward-looking statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

Although forward-looking statements contained herein are based upon what management believes are reasonable assumptions, forward-looking statements may prove to be inaccurate, as actual results and future events could differ materially from those anticipated in such statements. [The Company] undertakes no obligation to update forward-looking statements if circumstances or management's estimates or opinions should change, except as required by applicable securities laws.

# 目录

## CONTENT

<b>01 简介</b>	<b>2</b>
1.1 背景介绍	2
1.2 智能合约的核心问题	3
<b>02 OATH 概述</b>	<b>6</b>
2.1 简介	6
2.2 解决方案	7
2.3 仲裁机制	8
2.4 优势特点	10
2.5 工作流程	12
2.6 案例场景	16
<b>03 OATH 技术构架</b>	<b>18</b>
3.1 技术构架	18
3.2 区块链方案	20
3.3 节点机制	22
<b>04 OATH 法官机制</b>	<b>24</b>
4.1 法官身份认证	24
4.2 法官属性信息	25
4.3 法官筛选算法	26
4.4 法官信用评级	28
4.5 法官参与仲裁的代币奖励	31
<b>05 OATH 代币机制</b>	<b>32</b>
<b>06 OATH 项目计划</b>	<b>34</b>
<b>06 OATH 团队及顾问</b>	<b>35</b>
<b>07 参考文献</b>	<b>49</b>



# 简介

## 背景介绍

区块链通过去中心化的核心价值，结合了计算机理论，算法，密码学，博弈论，经济学等创造了能让社会大众达成共识的特殊机制，给整个社会带来了全新的协作模式和商业机遇。而这样一个去中心化的，由普通人共同参与协作，管理，维护的自治型社区，需要非常完善的信任体系，严格的合作标准，和健全的保障制度。以太坊的出现为区块链提供了一个在区块链上合作交易的解决方案：智能合约。

智能合约能够极大的降低信任的成本，去除第三方介入和担保，减少交易过程中可能存在的中介费用，增加履行合约的速度和可靠性。通过这个部署在分布式的区块链网络中，无法篡改，无人监管，但能自动执行的‘合约’，让陌生的个体可以在区块链网络中进行交易和合作。在智能合约的设计和概念上，使用场景应该相当广泛，比如电商行业，保险业，房屋租赁，银行业，金融服务业，进出口，等等。尽管有更多的商业合作或交易会从线下纸质合约转到区块链的智能合约上。可智能合约出现至今仍然没有被广泛的接受和运用，很多传统互联网的产品或者线下的交易都没有因为智能合约的出现被改变或者提升。

# 智能合约的核心问题



## 合约编写难度大

目前的智能合约只能通过计算机语言来编写。大多数合约使用者都无法掌握复杂的计算机编程语言，也无法编写一个完整有效的智能合约，以至于智能合约的使用门槛极高。



## 无法有效验证真实性

大部分商业模式无法避免的会涉及真实世界的合作或者交易，智能合约无法有效的验证部分内容的真实性，造成合约面临大量欺诈和舞弊的情况。



## 智能合约局限性较大

智能合约是一个通过合约双方约定编写的智能程序，这就意味着智能合约仅能解决最初约定好的那些条款，无法应对合作交易过程中产生的各种纠纷。



## 缺少链上治理和仲裁机构

基于区块链去中心化的宗旨和构架下，一旦产生纠纷，合约双方将很难找到一个有公信力的第三方机构来进行仲裁。即使到传统的法院去申诉，也会因为智能合约这类新的商业合作，难以找到完善的制度和健全的法律法规来保护双方的利益。



### 难以追溯

由于区块链保护隐私的特性，智能合约的各方一旦出现纠纷，合约内容，证据，仲裁结果，都无从追溯。若出现合约欺诈，欺诈一方甚至可以随意变更身份再次进行欺诈。

以上的这些核心问题环环相扣，如不解决，智能合约将很难在各个应用场景中普及开来。

## 区块链电商C2C交易

甲方：出售奢侈品牌二手皮包 乙方：消费者

乙方通过某个电商平台找到甲方正在出售的二手皮包，通过智能合约交易，下单购买收货后乙方发现皮包不符合预期的品质，要求退货，而甲方坚持当时在商品描述和照片中已经表示该皮包的全部细节，并且标明此商品为二手8成新，不接受退货。双方各持己见，无法达成共识。

## 区块链智能保险业务

甲方：区块链医疗健康保险合约 乙方：投保者

乙方作为投保者和某个区块链健康保险业务签订了智能保险合约，当乙方向平台索要赔付时，理赔的真实性很难判断，去中心化的保险业务，没有专人负责认定客户的理赔需求是否符合保险条款，也无法认定索赔金额是否符合情况。

## 区块链房屋租赁

甲方：区块链房屋短租业务      乙方：租房者

乙方在某个区块链短租房平台租用了房屋，离开后房东发现电视机被损坏，要求赔偿。乙方表示并非自己造成损坏，拒不赔偿，由于没有中心化的客服调解，双方无法再责任认定和赔偿金额上达成共识。

## 区块链内容版权

甲方：区块链内容版权平台      乙方：版权方

某个IP被在一个区块链内容版权平台进行注册后，乙方发现该版权为盗版，自己为真实版权拥有者，向平台发起申诉，由于缺乏仲裁机制，无法认定双方诉求的真实性，无从判断。

## 日常口头协议

区块链预测机已经十分普及，大家通过预测及来做日常的娱乐性或预测性对赌，比如球赛结果，竞选结果，甚至天气。而结果的真实性来源变得非常重要，如何确定一些有争议的结果的真实性变得异常重要。

以上仅是部分有潜在问题的案例，还有更多的实际应用场景需要一个完善的智能合约系统和一个公平的担保仲裁机制来保护使用者的权益，也让区块链和智能合约能更快速普及，实际落地到现实的使用场景中。



# OATH 概述

## 简介

OATH 是一个为完善区块链的基础构架而产生的跨链底层协议，称为智能合约纠纷化解协议（Smart Contract Alternative Dispute Resolution Protocol）。通过去中心化众包的方式，招募来自社区的陪审员，通过一个全新的共识机制，常识共识（Proof or Common sense），利用社区陪审员各自的专业知识和常识来为区块链上的应用和合约做验证担保，同时解决区块链和现实世界的真实性认证，及智能合约纠纷化解。

OATH 智能合约纠纷化解协议将提供区块链上的各类生态一个快速高效，公平公正，且有延展性的仲裁机制。该协议能为区块链上的智能合约提供一个强有力的担保，如果不出现纠纷，有一个公平的第三方仲裁机构来为合约双方进行评判。从各方面提高智能合约的可靠性，也同时给各类应用提供了更完善的保护机制，

对使用者来说，OATH 将是一个保护消费者的后支出保险方案，一旦使用了OATH 协议，出现问题后OATH 平台上的社区陪审员将通过他们的投票评判让消费者得到一个公平公正的裁决。而对于区块链上的应用来说，OATH 将极大的提高他们的信誉度和公信力，确保所有的合约都有一个有公信力的第三方机构作担保，若出现问题也会及时作出公平的裁定。

OATH 利用有延展性的跨链底层协议，特殊的共识机制，去中心化的紧密社区，以及确保公平公正的核心的技术手段，将为区块链的链上治理做出极大的贡献。从而完善区块链的信任体系，让更多的应用能够实际落地，在区块链上发展出更多更有趣的新型商业模式。

# 解决方案

首先OATH 将推出智能合约编程语言的拓展库，让用户在编写智能合约或者区块链应用时提前约定纠纷化解的方案，和违约赔付协议。

同时推出图形化的智能合约编辑工具，降低智能合约的使用门槛，提高智能合约的使用几率和使用场景。通过提供常用的合约模板，比如电商交易，真实性认定，版权申请，OTC交易等。模板中将自动绑定了OATH 协议，包含纷化解的方案，和违约赔付协议等。所有通过OATH 图形化界面编写的智能合约都将自动获得OATH 协议的担保，并且提供可能出现的纠纷仲裁。

最核心的是OATH 将通过 ‘社区陪审团’ 来为使用了OATH协议的智能合约做担保，为合约纠纷做仲裁和化解。也将成为区块链上的新闻，事件，预测结果和现实世界的桥梁，为他们的真实性做出鉴定和评判。



# 仲裁机制

在判例法系中，陪审制是一个非常有区块链特性的制度。陪审员通常为12人，（具体各国制度略有不同）是从普通公民中随机抽选的，除去部分特殊职业，比如警察，军人，所有成年公民都可能被选为陪审员。法官参加的审理中，法官主持法庭上的程序进行，裁定异议等。法官在结束审理时，将对陪审员进行详细引导（instruction, charge）。此后，陪审团根据在法庭上了解到的证据以及法官的指引，在一个封闭的房间内进行评议，就事实认定以及对该事实适用的法律等问题做出裁定（verdict）。从裁决的内容来看，一般原则上，陪审团只需要告知原告胜诉或被告胜诉，或者在原告胜诉时告知赔偿金额等结论，即所谓一般判决（general verdict）。

值得注意的是，陪审团成员全部从非法律相关专业的普通公民中随机选取。绝大多数的案件中，陪审员无需特殊的专业知识和技能，通过诉讼双方的证据和辩论，结合陪审员个人的理解和认知，从各类信息中找到依据，给出自己的判决。因为陪审员从社会各类人群中随机选择，所以陪审团的组成非常多元化。来自不同背景不同领域的陪审员，对案件有着不同角度的解读，也会让判决结果的相对更公平。同时，随机选出的这些普通陪审员，在大概率上可以代表社会各类人群，他们达成的共识所给出的判决结果，可以映射到社会大多数人的共识，代表社会普遍认知。

整个陪审制度非常符合区块链的去中心化的民主思想，通过来自社区的所有参与者，共同接受的一个相同的共识机制，通过大多数人共同决策来进行判决。所以，OATH 众裁链希望通过效仿判例法系中的陪审团制度，配合区块链技术，加密算法，智能随机算法，信用评级，案件追踪等技术，创造一个智能合约的纠纷化解机制。由来自不同背景，不同专业的社区陪审员（OATH Jury），来为合约进行担保，裁决可能发生的合约纠纷，通过合约内容，证据，证词，辩论，等因素做出裁决。

区块链技术的特性将确保智能合约的内容真实可靠，双方提供证据不会被篡改。通过加密技术将 OATH 陪审员的身份严格保密，使得他们做出的裁决不会受到任何外部的影响。同时给 OATH 陪审员设定了大量细致的分类（Categories），比如性别，年龄，国籍，

语言，职业，学历，等。配合智能随机算法，保证纠纷仲裁时所选取的陪审员来自不同的领域，拥有不同的背景，减少偏见。同时利用信用评级（Credit Level），来评估和限制陪审员的行为，陪审员会通过做出合理公平的裁决获得更高的信用评级，从而获得更多的回报。相反的，连续多次做出错误判断的陪审员将损失信用评级，到一定的程度后将无法继续参与仲裁。在越来越多的陪审员参与到合约纠纷的仲裁中，OATH 将对陪审员建立关系属性（Attributes），以减少同类型陪审员共同参与案件的数量，保证陪审员的多元化和提高仲裁的公平性。

纠纷解决的过程中也将不同于传统的法院，合约双方将拥有更多的自主权，可以设定仲裁的条件，比如所需陪审员的数量，胜诉所需要的投票数量，和双方所需要的陪审员类别。裁决结果也会公开透明，陪审员的类型，投票结果和投票理由都会在结果出现后对所有人公开，若有任何异议也可以随时提出上诉。在案件结果出现后，案件的详细内容和投票结果也会加密保存。OATH 也会为案件做出归类索引，在确保隐私的前提下，提供后续查阅。



# 优势特点



## 合约担保

一个公平公正的智能法庭能为区块链和智能合约做一个可靠的背书，确保合约出现纠纷后一定可以得到合理的解决。这样区块链和智能合约的可靠性将大大提高。



## 迅速高效

一旦出现纠纷，在双方已经选择了OATH法庭的前提下，合约中任何一方签名确认，OATH 智能合约纠纷仲裁案就会自动生成。无需额外的流程。之后双方会有5天的时间提供相关证据，OATH 法官们会在证据提供完成后的3天内做出裁决。在没有申请延长或上诉的情况下仅需8天就能产生裁决结果。



## 公平公正

OATH 利用区块链的开放性和可靠性，首先确保案件的内容无法篡改，其次利用加密技术将法官的身份严格保密，再加上智能的随机算法，保证每个案件所选择的法官们能来自不同的领域，拥有不同的背景。同时 OATH 提供了合约双方更多的权利，可以设定仲裁案件的细节，比如：

- \* 仲裁需要的法官数量（单数，11–51名）
- \* 获胜方所需要获得的投票百分比。（51% – 100%）
- \* 所需法官的类别。（性别，年龄，国籍，语言，职业，学历，信用等级，等。）

在投票的过程中，法官和合约双方都无法看到投票的进程。当结果出现后，所有投票信息和投票理由都将被公开，保证结果的公开透明。若对结果又异议，可以提出上诉，上诉案件中前一次的裁决结果不会被公开，确保新进法官不会存在偏见，而上诉结果也将纳入对法官的信用评价体系中。



## 成本可控

合约双方在编写智能合约时将需要为纠纷仲裁计划抵押一些 OATH 代币，这些代币将成为可能出现的合约纠纷案件的仲裁费用。若合约顺利完成，这些货币将全数退还给合约双方，没有任何额外的费用。但若合约出现纠纷，仲裁费用会在仲裁结果出现之后，按比例分配给所有做出正确选择的法官。

OATH 为确保法官有意愿来审理案件，会在选取法官后，将仲裁费用和其他基本信息通知法官，他们可以通过这些信息来选择是否接受案件。若仲裁费用的数额过低，没有足够的法官愿意接受案件，OATH 允许合约双方抵押更多的代币，吸引更多法官，或降低要求法官的数量。所以仲裁的费用成本非常可控而且经济实惠。



## 有效执行

在双方编写智能合约时，可以提前在智能合约仲裁计划中编写违约赔偿方案。若出现合约纠纷，并出现仲裁结果且双方签字确认后，OATH 会自动将仲裁结果回传到智能合约中，合约将继续按照双方先前定义的规则，终止交易或者继续进行交易。

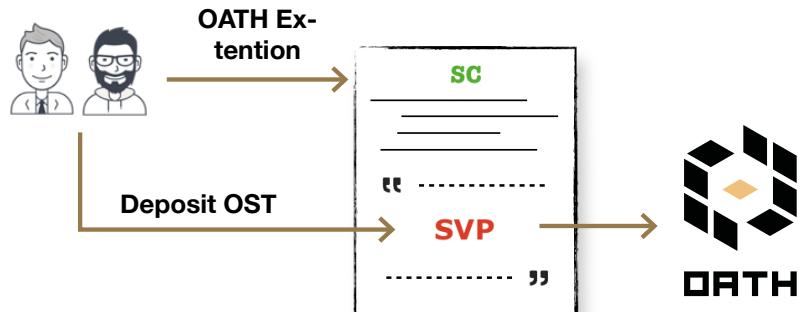


## 记录案件

区块链的整体框架是保护使用者的隐私，无从得知使用者的身份。OATH 将基于隐私保护的前提下，将智能合约纠纷案件的内容加密后存储在 OATH 区块链中。将来可以通过案例回溯的方式找到曾今发生过的“案件详情”。这样可以从侧面提高智能合约的安全性，让更多的智能合约使用方有办法了解曾经发生过的纠纷，让法官和其他相关人士能够了解过去案件的裁决结果。

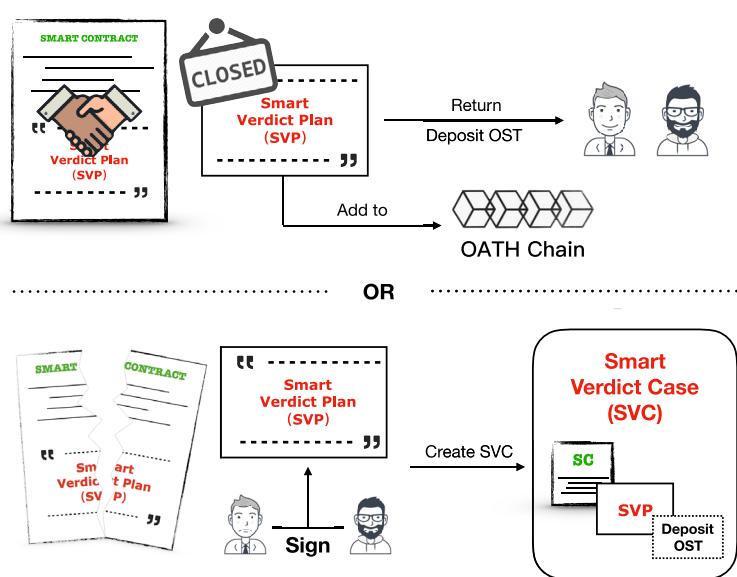
# 工作流程

01



OATH 对目前主流智能合约的编程语言进行拓展，通过 OATH 提供的 API，合约双方在编写智能合约时可以添加纠纷仲裁的计划（ Smart Verdict Plan, SVP ）和若出现纠纷后的协议方案等。双方在 SVP 中需要抵押一定量的 OATH 代币（ OST ），作为出现纠纷后的仲裁费用。

02



智能合约部署后，  
OATH 会监听合约  
进行情况。若合约  
顺利完成，则 SVP  
会被自动关闭，同  
时将先前抵押的  
OST 全部还给合  
约双方，并将 SVP  
信息加密后保存到  
OATH 的区块链

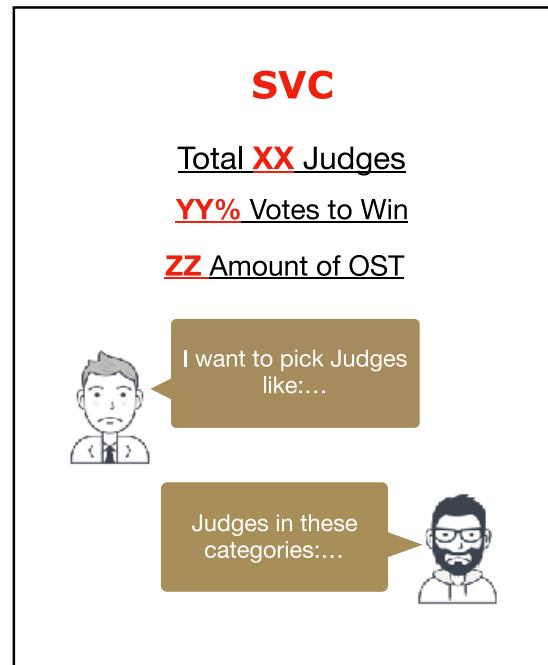
中。

若出现智能合约纠纷，合约任意一方签名后，OATH 将把 SVP 自动转化成智能合约纠纷仲裁案（ Smart Verdict Case, SVC ），同时把先前抵押的 OST 作为 SVC 的仲裁费用，与合约内容一并带入 SVC 。

## 03

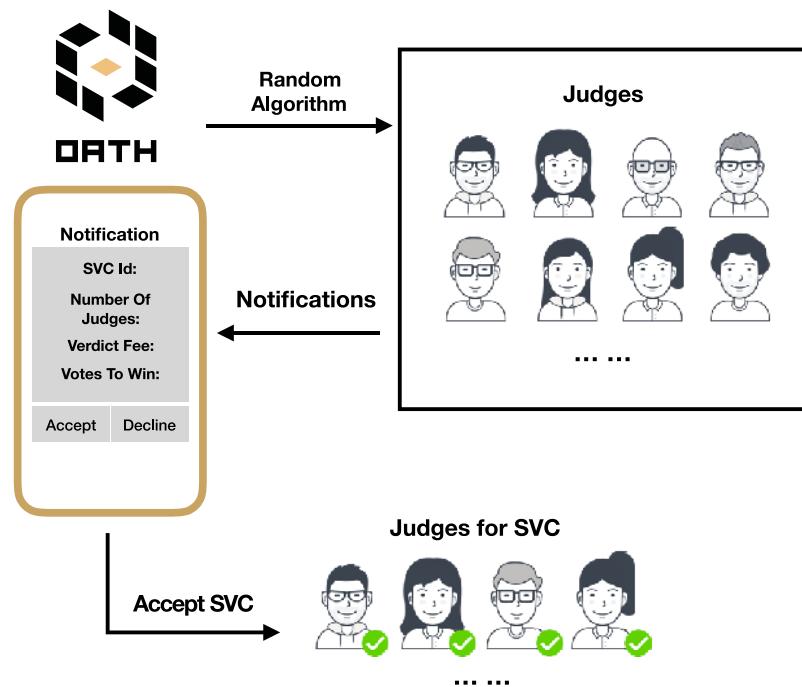
SVC建立后，合约双方可以设定仲裁细节：

- 仲裁需要的法官数量（11–51人，单数，默认11人）
- 获胜所需要的投票百分比（51%–100%，默认51%）
- 仲裁费用（默认为SVP时抵押的数量）
- 双方各自所需要的法官类型（性别，年龄，国籍，语言，职业，学历，法官信用等级，等）



SVC 的设置完成后内容将被加密保存到 OATH 的区块链中。

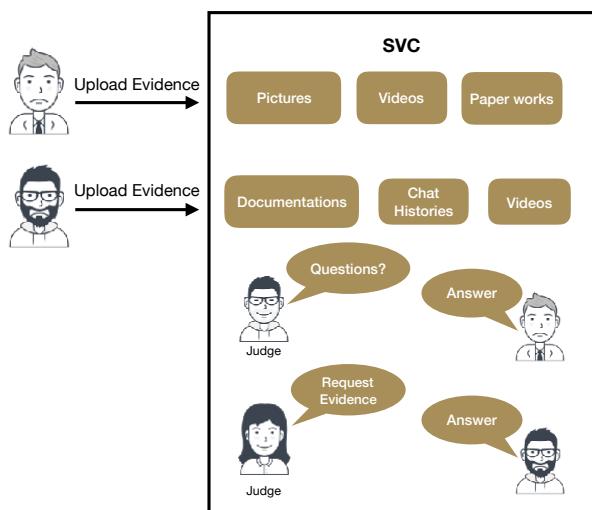
## 04



当 SVC 设置完成后，OATH 通过分类随机算法（Categorizing Random Algorithm），根据法官的类别（Categories）和法官的关系属性（Attributes），随机选择出设定数量的法官。其中三分之二的法官将符合合约双方设定的类别（双方各三分之一，若完全符合要求的法官数量不足，则用部分符合的法官填补），剩下三分之一将通过 OATH 的算法随机选择，且错开双方规定的类别。

OATH 会选择所需数量两倍的符合要求的法官，并发送推送通知。通知中包含 SVC 的基本设定，比如所需法官的总数，获胜所需的投票百分比，仲裁的费用等。法官可以按照这些信息来决定是否接受案件。OATH 将采取先到先得的方式，所需三大类（合约双方和 OATH 平台方）法官数量分别达到后，剩余该大类法官将无法接受案件。若没有足够的法官愿意接受案件，OATH 允许合约双方修改SVC的设置，抵押更多的代币，或降低要求法官的数量等等，来吸引更多法官。

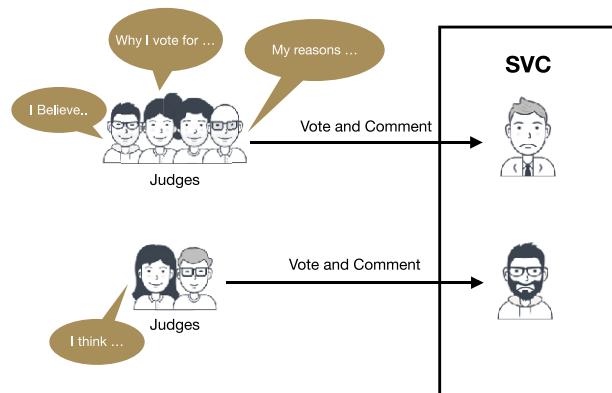
## 05

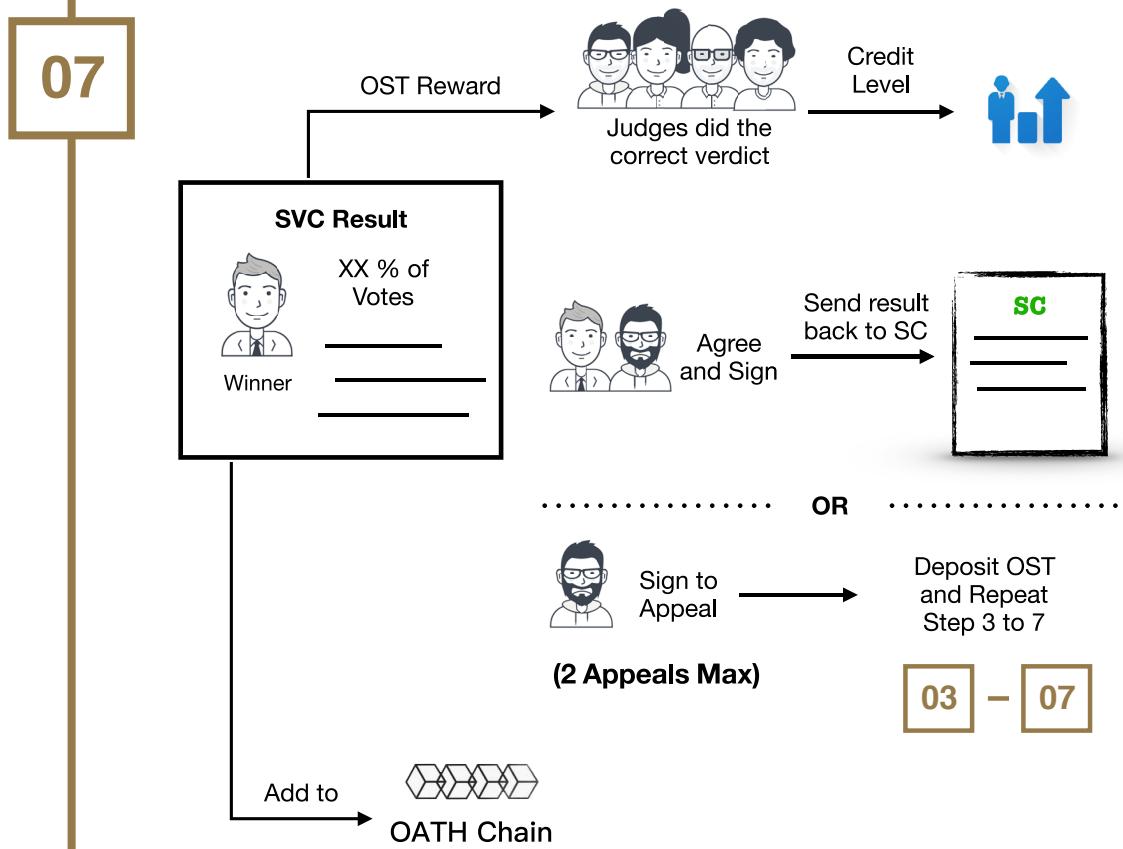


随后双方将有五天时间上传各自持有的相关证据（文字，图片，视频，等），若需要更多时间可以单方面申请延长，申请延长时需要选择相应的时间并抵押同比例的代币，比如5天则需多抵押100%的 OST。法官们可以在证据阶段中提出自己的问题，或者索要更多的证据，OATH 社区将对提出合理问题的法官在进行一定代币和信用等级奖励。鼓励法官能提出关键性的问题、带动案情讨论进程。在过程中法官的身份会被严格加密，确保法官不会受到外界的干扰。

证据阶段结束后将进入3天的仲裁投票，法官在投票后可以附上投票的理由。为确保案件仲裁的公平性，在投票结果出现前，法官和合约双方都无法看到投票情况。

## 06





当仲裁结果出现后，每位法官的投票结果和理由将被公开展示，同样的法官的身份会被严格加密。合约双方和其余法官能更好的理解仲裁的结果和原因。

仲裁费用将按照信用等级公式加权分配给所有做出正确仲裁的法官们。做出正确仲裁的法官们同时将获得信用等级的奖励。

合约双方在仲裁结果出现后，5天内必须签字认可或提起上诉。若双方均已签字认可或在规定时间内没有提起上诉，则仲裁结果会被发送回智能合约，按照合约约定内容继续执行。

若提起上诉，则仅需单方面签字，并支付代币作为新的仲裁费用，OATH 将开启一个新的SVC，重复上述步骤3至7。为了确保公平，上诉的SVC中将不包含之前SVC的结果。且上诉案件中仲裁费用和法官的信用等级将有一定的限制，仲裁费用将不得低于前一次的仲裁，法官的平均信用等级也将高于前一次，更多有经验的法官将参与给出判决。一个SVC的上诉为1次。上诉结果将被自动回传给智能合约。

## 案例场景

OATH 所提供的仲裁服务适用面非常广泛，任何可能产生纠纷的商业合约都可以使用。比如有常见的电商服务，C2C或B2C，OATH 都可以充当去中心化的售后纠纷仲裁。或存在任何不对等风险的商业交易，比如加密货币的场外交易，区块链房屋产权交易，等等。或任何需要仲裁机构来介入的第三方服务，比如保险理赔业务，民事诉讼案件等等。

### 电商C2C纠纷案件仲裁

甲方：出售奢侈品牌二手皮包      乙方：消费者

乙方通过某个电商平台找到甲方正在出售的二手皮包，通过智能合约交易，并添加了 OATH 的纠纷计划作为担保。下单购买收货后乙方发现皮包不符合预期的品质，要求退货，而甲方坚持当时在商品描述和照片中已经表示该皮包的全部细节，并且标明此商品为二手8成新，不接受退货。双方产生纠纷。

由于在先前的智能合约中使用了 OATH 的拓展，并且添加了纠纷化解计划，和描述清楚了赔偿方案，如果甲方获胜，则乙方需确认收货，将钱款转到甲方账户，若乙方获胜，则甲方需要接受退货退款。所以仅需其中一方签字后，SVC 仲裁案件就会被创建，随后甲乙双方约定需要21名法官，超过60%投票获胜，法官没有特殊类别。

之后进入举证阶段，甲方将之前的货品描述，图片，和乙方的聊天记录全部上传到证据池中，并且写下陈述表示之前的商品中已经完全描述清楚商品的新旧程度，并且图片中已经清楚标明有问题的地方，乙方则拍摄商品的视频和照片上传到证据池中。

法官通过双方的证据和陈述进行投票后，超过60%的法官选择了甲方获胜，并且大部分法官都留下投票理由为甲方描述和商品属实，无需承担退货责任。双方确认结果后，OATH 将结果回传到智能合约，合约自动将商品费用转至甲方。

## 新闻事件的真相判定

甲方：想了解真相的群众

当某个重要的新闻事件出现后，各种各样的消息和所谓的真相让整个事件的变得非常模糊，且随着事件的发展，焦点容易被模糊，真相反而被谣言所掩盖。甲方作为想了解的群众可以使用 OATH 平台发起对某个新闻事件的真相追溯，希望大家来提供某个事件的证据和真相。甲方在OATH 平台开启新闻事件真相追溯案件 SVC，抵押一定的货币做为证据搜集和法官的奖励，设定正反双方的观点，随后 OATH 用户可以提供正反双方的各类证据，同时选择一定数量的法官来通过各类用户提供的所有证据对事件的真相进行判断。

## 区块链保险理赔仲裁服务

甲方：区块链医疗健康保险合约

乙方：投保者

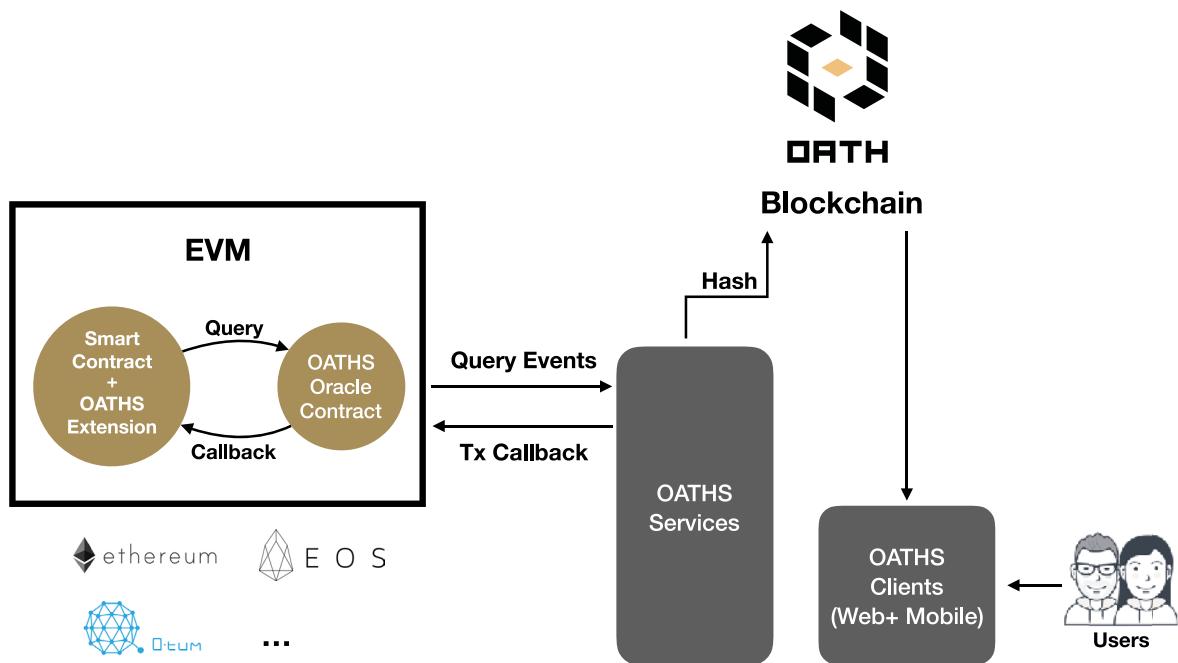
在未来的区块链去中心化的格局中，区块链保险业务一定也会一定程度的受到关注。基于目前的区块链技术和框架下，去中心的保险业务理赔的判断一定是通过去中心化方式的仲裁。所以 OATH 可以完美切合区块链保险业务，成为公平且高效的保险业务中的理赔仲裁服务。

乙方作为投保者和某个区块链健康保险业务签订了智能保险合约，其中约定使用 OATH 平台作为仲裁机构，确保在理赔发生时能有明确的判断，是否符合保险条款。乙方若出现任何需要理赔的问题，可以直接发起一个 SVC, 通过上传自己的相关证据和诉求，而智能保险合约内容会被当做甲方的证据自动加入 SVC，所有法官可以通过双方的保险条款和乙方的诉求来决定是否通过理赔。



# OATH 技术构架

## 技术架构



由于智能合约是在虚拟机执行，是一个封闭的环境。合约无法和外界直接通信或取得任何资料。而 Oracle 预言机的就是为区块链智能合约提供可信的链外数据，用来触发智能合约顺利执行的数据来源。Oracle 可以通过监听特定的 Event 来接受合约所发出的 Query, 处理完成之后再由 Oracle 主动呼叫合约的回调方法将资料传回。所以 OATH 服务将使用 Oracle 完成公链和 OATH 平台之间的一系列服务。

OATH 将在主流公链（比如以太坊，量子链，EOS，等）上部署 OATH 的智能合约拓展（OATH Extension），里面包含了 OATH 提供的智能合约纠纷仲裁相关的API。同时在公链上建立 OATH Oracle 智能合约，作为公有链上智能合约和外部 OATH 的服务的中间沟通桥梁。

当一个引用了 OATH 扩展，并编写了智能合约纠纷仲裁计划（Smart Verdict Plan, SVP）和其他相应协议的智能合约，成功部署到公链或接收到纠纷仲裁相关指令后，智能合约会发送相应 Query 到 OATH Oracle 智能合约。通过 OATH Oracle 智能

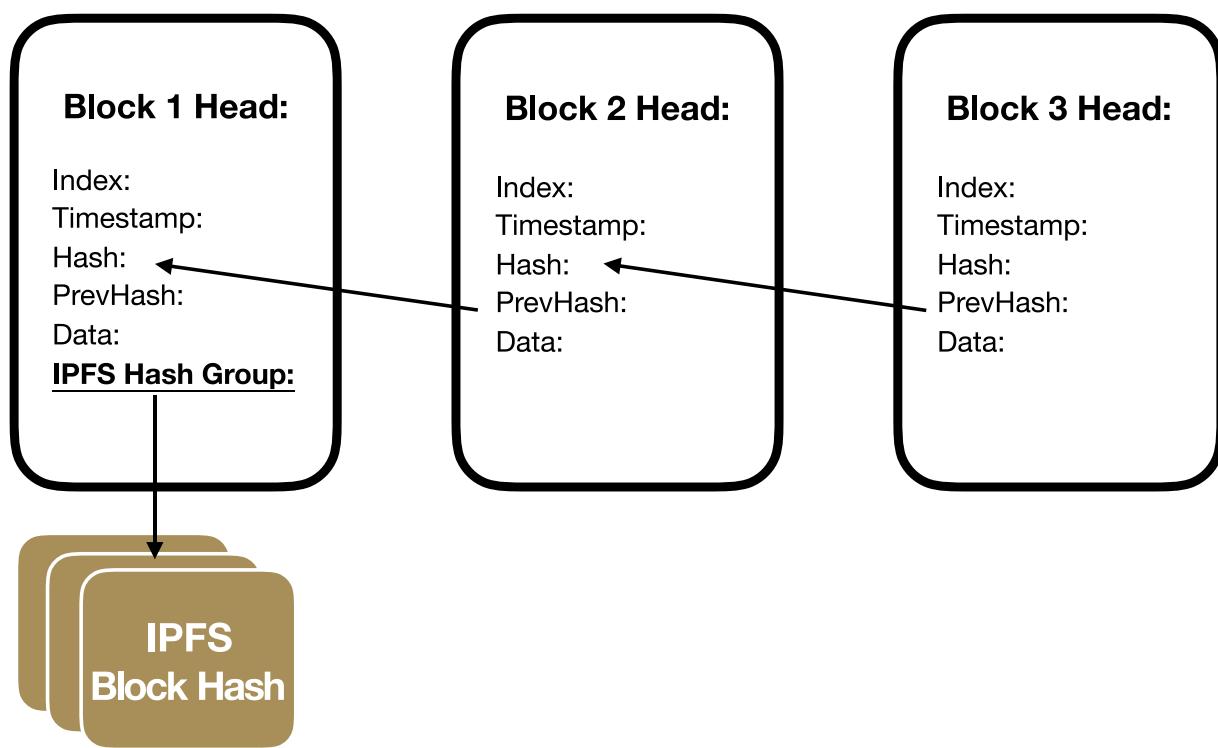
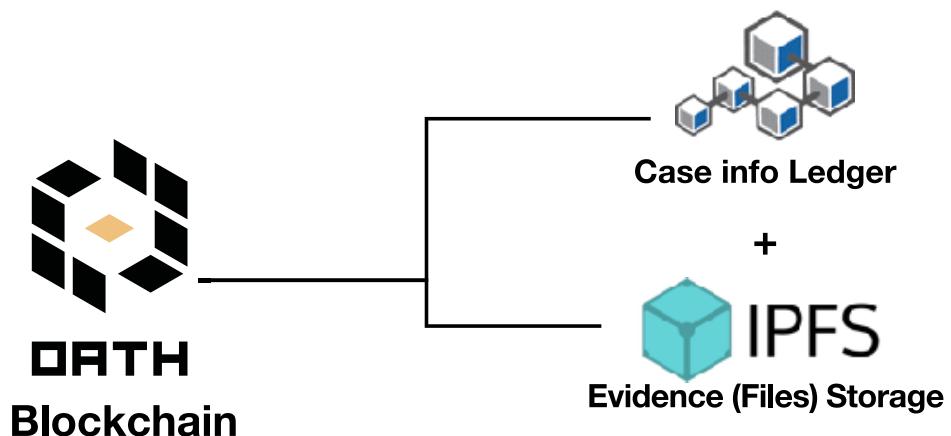
合约发出相关的 Query Event。OATH 的服务在监听的过程中接受到了Event的请求之后，会将相应的信息加密保存到 OATH 的区块链中，（比如建立仲裁计划，开启仲裁案件，等）。如果涉及到数据回传（比如仲裁结果等），利用 OATH 的外部服务向 OATH Oracle 智能合约发送数据，然后通过该智能合约转发到用户的智能合约上。

OATH 为确保信息可靠安全，数据提供了基于 TLSNotary 的可信证明技术。TLSnotary 证明主要基于安全传输层协议TLS 1.1，TLS 用于在两个通信应用程序之间提供保密性和数据完整性，最大优势就在于独立于应用协议，更高层协议可以透明地分布在 TLS 协议上面。

TLS包含三个基本阶段：1.对等协商支援的密钥算法；2.基于私钥加密交换公钥、基于PKI证书的身份认证；3.基于公钥加密的保密数据传输。在整个传输中，TLS 的 master key可以分成三个部分：服务器方、受审核方和审核方。在 OATH 流程中，OATH 节点所给出的数据源作为服务器方，OATH 服务作为受审核方，一个专门设计的，部署在云平台上的开源实例作为审核方，每个人都可以通过这个审计方服务对 OATH 过去提供的数据进行审查和检验，以保证数据的完整性和安全性。



# 区块链方案



OATH 的区块链中将有两条平行的私链配合完成所有需要的功能。首先是一条主链，案件信息账本，用于保存所有案件相关的信息，比如合约内容，投票结果，投票原因，参与法官，等等。其次，OATH 会部署一条私有的IPFS链用于存储案件相关的证据文件，以确保证据文件的安全性和不可篡改性。

IPFS ( InterPlanetary File System ) 是一个点对点的分布式超媒体分发协议。IPFS用内容地址替代传统的域名地址，用户不用考虑文件存储的名字和路径。将文件放到IPFS

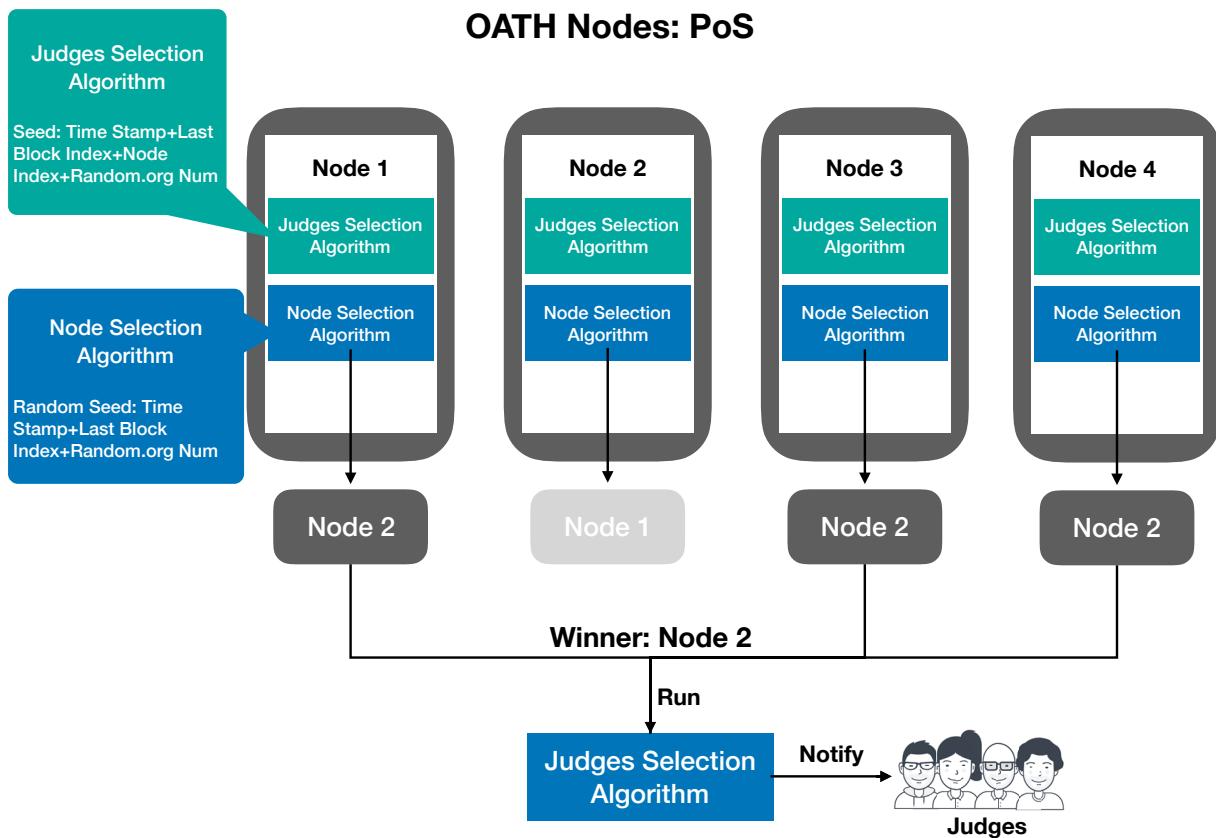
链上，会得到基于其内容计算出的唯一哈希值。哈希值直接反映文件的内容，哪怕只修改1比特，哈希值也会完全不同。当IPFS被请求一个文件哈希时，它会使用一个分布式哈希表找到文件所在的节点，取回文件并验证文件数据。IPFS是通用目的的基础架构，基本没有存储上的限制。大文件会被切分成小的分块，下载的时候可以从多个节点同时获取。IPFS的是不固定的、细粒度的、分布式的网络，可以很好的适应内容存储和分发的网络的要求。

在案件信息账本中的区块里若涉及到证据信息，会额外有一个IPFS Hash Group的数据，其中就包含了所有该案件相关的证据文件的IPFS Hash Key。IPFS中存储的文件的密钥（Private Key）将通过加密算法生成，而算法内容将不对外公开，以确保文件的安全和私密性。

而案件信息将由数个关联链接的区块共同构成，比如：

1. SVP 区块，其中包含了加密后的合约内容，抵押货币，合约双方钱包地址，等信息；
2. SVC 区块，其中包含了 SVP 区块的哈希值，加密后的案件的法官信息，案件证据的 IPFS Hash Group，等信息；
3. SVC 仲裁结果区块，其中包含了 SVC 区块的哈希值，加密后的投票结果，投票过程，等信息。

# 节点机制



OATH 的节点采用权益证明（Proof of Stake, PoS）的共识机制。每个节点将负责记录案件的信息，存储证据文件，和 OATH 的外部服务，比如 Oracle Query Event 监听服务，法官筛选算法，等。

OATH的节点监听服务将监听部署在公链上的 OATH Oracle 智能合约所发出的 Query Event，通过 Query Event 中所包含的信息来进行相对应的操作。所有的节点都将共同监听，收到 Event 信息后会和附近的节点进行对比和确认，一旦超过半数以上确认无误之后会开始运行节点随机筛选算法（Node Selection Algorithm），用当前的时间戳（Timestamp）加上最新的区块的Index和Random.org所提供的可信的随机数，作为随机算法的种子，通过加入Random.org所提供的随机数来确保随机种子不可预测，保证安全性。然后每个节点会算出一个节点的编号，获得最多选择的节点将被选为当前的记账节点。负责将相应的信息记录到区块链上。若遇到出现超过一个最多选择时，则以更靠前的节点优先。

比如当 OATH 需要对选择某个案件的法官时，首先通过节点随机筛选算法，选择出当前的记账节点，然后通过部署在节点上的法官筛选算法，使用时间戳，节点编号，最新区块的Index 和 Random.org 提供的随机数作为算法的种子，运行法官随机算法。获得结果后，其他节点运行进行验证比对，通过验证比对后，将法官信息记录到区块链上，同时向法官发起推送。

OATH 面向用户的客户端将有网页和移动两个版本，主要负责案件展示，案件创建，证据上传，投票，结果展示等。移动软件将有安卓和iOS两个版本，可以让用户更便捷的收到案件推送通知，实时的保持对案件的关注。



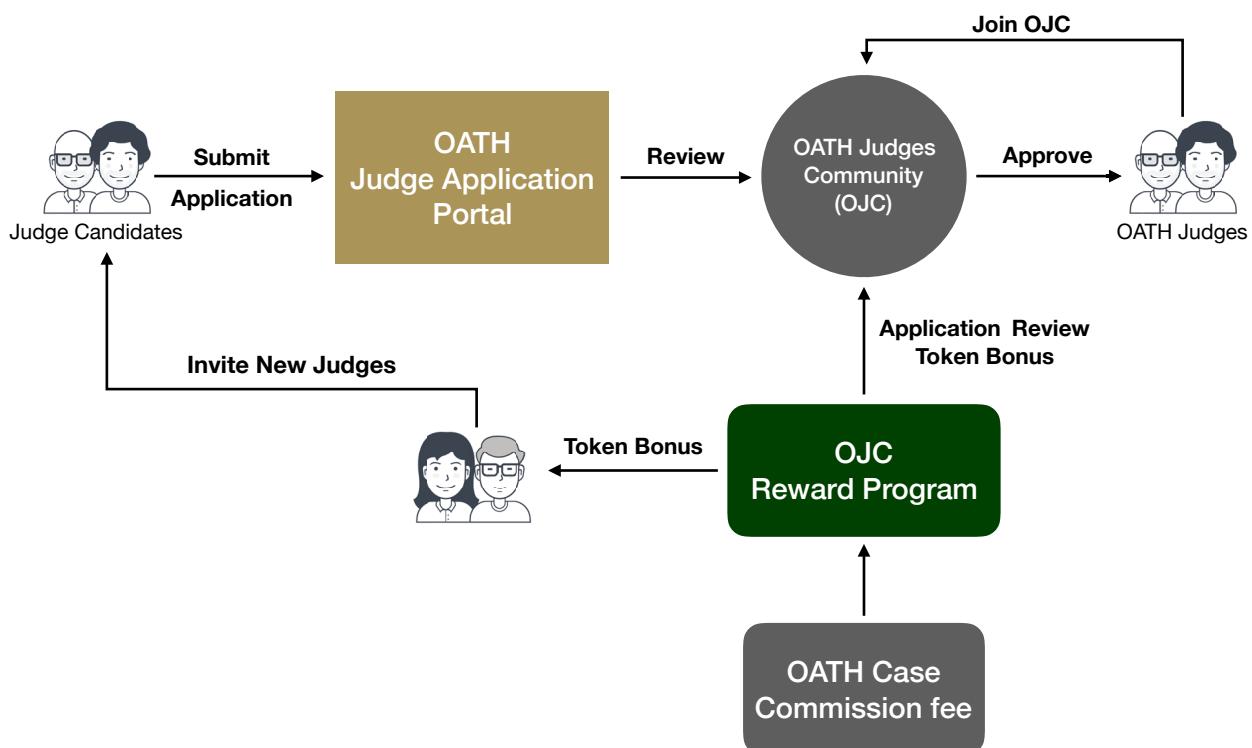


# OATH 法官机制

## 法官身份认证

为了确保 OATH 法官能够提供公平合理的仲裁，OATH 初期会谨慎审核法官的资质和身份。用户可以通过 OATH 的客户端申请成为法官，需填写详细个人信息，比如性别，年龄，国籍，语言，专业背景，职业等等。OATH 团队中的法官社区管理团队（OATH Judges Community, OJC）会通过人工审核的方式通过所有申请，同时会根据法官的背景给法官设初始信用等级。

为了奖励和鼓励法官填写详细的个人信息，法官通过人工审核后，OATH 会给与一定的起始奖励期限，例如前5个案件，法官将获得额外50%的代币奖励，来自于社区的运营的代币池。



当法官数额超过一定数量后，法官身份审核将交由社区自行审理。OATH 将随机筛选信用等级较高的法官来审核新法官的背景和身份，通过投票通过的方式进行身份审核，并通过综合评分的方式来决定法官初始信用等级。进行身份审核的法官将获得社区代币奖励。

OATH 也允许信用等级较高的法官来推荐新法官，当被推荐人通过身份审核，并成功仲裁一定数量的案件后，推荐人和被推荐人都将获得社区的代币奖励。

## 法官属性信息

OATH 的每位法官都会有两种属性数据，分类属性（Categories）和关系属性（Attributes）。分类属性的目的是将法官的个人信息标签化，用于更分散随机的筛选和更合理的归类。而关系属性是随着法官的仲裁和平台发展过程中变化的，用于大幅度避免可能存在法官串通或舞弊，让案件获得更公平和可信的仲裁。

法官的分类属性其中包含了：年龄，性别，国籍，语言，专业，职业，学历，等等的一些静态的个人信息。OATH 致力于让来自不同领域，不同背景的法官共同参与到纠纷仲裁中。让法官们从不同的领域，不同的观点，不同的角度来进行案件的仲裁。保证纠纷案件能够获得到来更广泛人群和更有代表性的结果。大多数的法官所作出的共同选择会成为纠纷仲裁的结果，所以让到来自不同背景的法官达成共识才能确保案件的公正性。用户在申请成为法官时就需要填写相应的分类属性，法官也可以通过申请修改来调整分类属性，而修改内容则需要通过法官社区来审核通过。

法官的关系属性是动态变化的关系图谱，随着法官参与更多的纠纷仲裁，关系属性会动态的变化。每次纠纷仲裁后，OATH 会记录所有参与该纠纷仲裁的法官，结合纠纷类型，成为法官的最新关系图谱。在 OATH 法官筛选算法中会优先选择符合分类的且没有关系属性的法官，将尽量避免法官“连续共同”参与纠纷仲裁，以避免潜在的法官串通舞弊。

# 法官筛选算法

OATH 对于法官筛选时将采用 Fisher-Yates 洗牌算法，Fisher - Yates 洗牌算法是由 Richard Durstenfeld 在1964年 描述。并且是被 Donald E. Knuth 在《The Art of Computer Programming》 中推广。他是一个用来将一个有限集合生成一个随机排列的算法（数组随机排序）。该算法每次随机选取一个数，然后将该数与数组中最后或最前的元素相交换，如果随机选中的是最后/最前的元素，则相当于没有发生交换；然后缩小选取数组的范围，去掉最后的元素,即之前随机抽取出的数。重复上面的过程，直到剩余数组的大小为1，即只有一个元素时结束。这个算法生成的随机排列是等概率的。同时这个算法非常高效。

OATH 先将所有的法官通过 Fisher-Yates 算法形成一个随机的序列; 第二步遍历该序列，将法官按照合约双方指定的条件放入对应的bucket和系统随机的bucket (共三个bucket)。仲裁双方的条件不一定是完全互斥的，所以存在一种情况即：该法官同时满足双方的条件。在这种情况下，优先把该法官放到容量较小的那个bucket，如果两个bucket容量相同，则放到第一个bucket。如果不满足双方的条件，放入系统选定的bucket，如果三个bucket都已满，退出法官选择算法。

以下为算法的伪代码

```
1. let a := array_of_judges
2. let n := a.length
3.
4. struct bucket {
5.     data; // judge bucket array
6.     func; // function returns true if the given judge fits
       the requirement for this bucket
7. }
8.
9. // Phase-1 Fisher-Yates shuffle
10. for i from n-1 down to 1 do
11.     j ← random integer such that 0 ≤ j ≤ i
12.     exchange a[j] and a[i]
13.
```

```
14. // Phase-2 Bucket filling
15. let fulfilled := false
16. for i from 0 up to n-1 do
17.     If bucket_1.is_full() and bucket_2.is_full() and bucket
        _3.is_full():
18.         fulfilled = true
19.         break

20.     If (not bucket_1.is_full()) and bucket_1.func(a[i]):
21.         bucket_1.data.append(a[i])
22.
    else if (not bucket_2.is_full()) and bucket_2.func(a[i]):
23.         bucket_2.data.append(a[i])
24.     else if not bucket_3.is_full:
25.         bucket_3.data.append(a[i])
26.
27. // Phase-3 final check
if not fulfilled:
28. throw exception("No sufficient amount of judges for this el
ection")
```

算法复杂度为O(N)，即和法官数量成正比。

# 法官信用评级

法官信用等级（ Credit Level）是 OATH 平台用于激励和评价法官的信用体系。OATH 利用信用等级代替传统的货币抵押方式，为鼓励法官在纠纷仲裁中做出更确切合理，公平公正的判决。更高的信用等级将获得更多的加权货币奖励。

OATH 将法官设定为20个不同的等级。所有法官在刚加入 OATH 平台，并通过身份审核后，OATH 将根据法官个人背景综合评分获得初始信用等级（1级至5级）。

法官信用等级可以可通过积极参与纠纷仲裁和做出更多正确的选择（投票给了纠纷的胜诉方）来获得信用积分，达到一定积分后，法官信用等级将自动提升。法官信用等级与信用积分的关系表达如下：

$$L = 1 + \sum_{i=1}^n \epsilon \left( P - \left( 1 + \sum_{j=1}^i Fibo(j) \right) \right)$$

其中L为法官的信用等级  $L \in [1, 20]$ ，P为法官的信用积分， $\epsilon(t)$  为标准阶跃函数，符合标准节约信号的描述，Fibo为斐波那契数列。

具体的信用等级经验值表如下表：

信用等级	信用等级对应的信用积分/奖励系数	信用等级提升所需积分
1	1	1
2	2	2
3	4	3
4	7	5
5	12	8
6	20	13
7	33	21
8	54	34
9	88	55
10	143	89
11	232	144
12	376	233
13	609	377

<b>14</b>	986	610
<b>15</b>	1596	987
<b>16</b>	2583	1597
<b>17</b>	4180	2584
<b>18</b>	6764	4181
<b>19</b>	10945	6765
<b>20</b>	17710	

信用积分的变化由每个纠纷仲裁中多个因素共同决定：

1. 本次仲裁的结果：法官的投票将直接影响信用积分的增减。法官成功投票给了胜诉方，法官将获得2点信用积分。反之投票给了败诉方，则将减少2点信用积分。  
且为维持平台的公平和稳定，连续做出错误选择的法官的信用积分将大幅度降低。
2. 纠纷仲裁时间：对纠纷仲裁案的反馈和决策速度也是对法官的重要衡量指标。在规定时间内做出仲裁是法官的重要职责，法官在超过规定时间不做出裁决将视为弃权，任何弃权都可能影响案件的效率和结果。在规定时间内做出裁决的法官将获得1点信用积分，而超时的法官将扣除2点信用积分，连续放弃的法官将以加权的方式扣除信用。
3. 上诉的结果：纠纷仲裁案的上诉情况也将会影响本次纠纷涉及仲裁者的经验值。若上诉维持原结果，则说明法官做出了非常公正的裁决，将会获得额外的1点积分。若上诉结果改判，则原先的法官做的裁决对合约纠纷产生不良的影响，法官则会受到加倍的信用积分惩罚，扣除3点积分。原判做出正确选择的法官，会得到本应得到的2点信用积分。

### 例如：

法官 Bob 参与了一次纠纷仲裁，做出了正确的选择。Bob 则获得了2点信用积分。并在规定时间内做出了选择，获得了决策时间奖励1点信用积分。则这次仲裁 Bob 共获得3点信用积分。

假设这个纠纷案件被提起上诉，新的诉讼将选择新的一批信用等级更高的法官，Bob 虽然无法参与，但上诉结果若维持了Bob原来的判决，他将获得额外的1点信用积分奖励。最后他参与这次纠纷的总共获得4点信用积分。

法官每一次仲裁后的获得信用积分  $p_i$  为：

$$p_i = P(R(r_i), T(t_i), C(c_i))$$

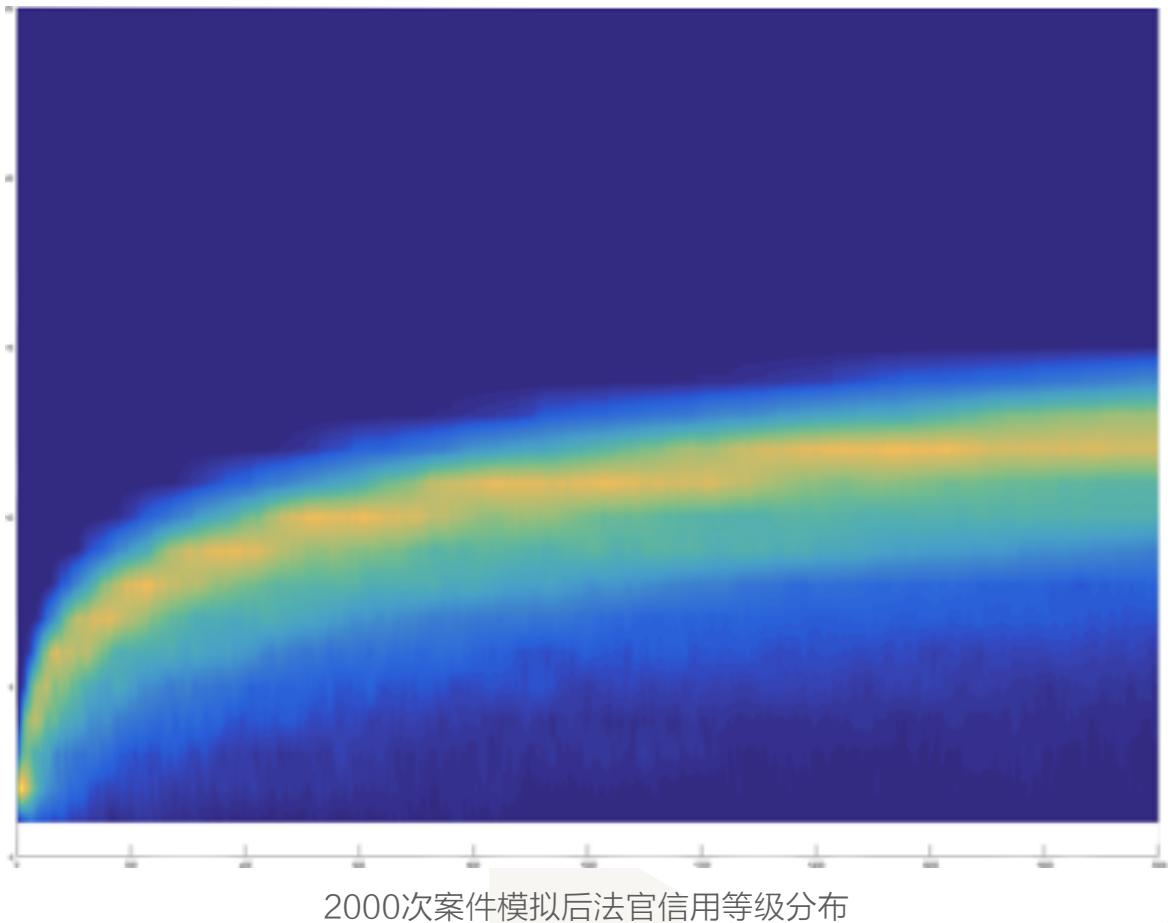
$R(r_i)$  为与该次仲裁的结果对应的信用积分函数

$T(t_i)$  为与该次仲裁的决策时间对应的信用积分函数

$C(c_i)$  为与该次仲裁上诉情况对应的信用积分函数

法官的累计信用积分为：  $P_{total} = \sum P$

为了提高 OATH 平台的可玩性和持久性，我们模拟了 2000 次纠纷仲裁后法官的等级分布。大部分的法官将在 5-15 级之间，随着等级的提高，升级的难度也会大幅度提高。



## 法官参与仲裁的代币奖励

法官的信用等级是专业性和积极性的证明。为激励法官获得更高的信用等级，积极参与 OATH 平台上的各类纠纷案件，所以法官的信用等级越高，参与仲裁后获得仲裁费用比例也越高。在 OATH 平台以法官的信用积分作为仲裁费用分配的系数，具体的分配方式如下：

$$R_j = Fee \times \frac{S_j}{\sum_{i=0}^n S_i}$$

其中Fee为该次纠纷仲裁的总费用， $S_j$ 为第 j 个仲裁法官当前的信用积分， $R_j$ 为其在本次仲裁中获得的仲裁费。

为激励法官社区的成长，早期的参与者将获得更多的经验值，同时获得更多的回报，随时社区的增长和扩大，早期参与者将参与到社区的维护和管理中，确保 OATH 的仲裁机制能够长久稳定顺利的运行。



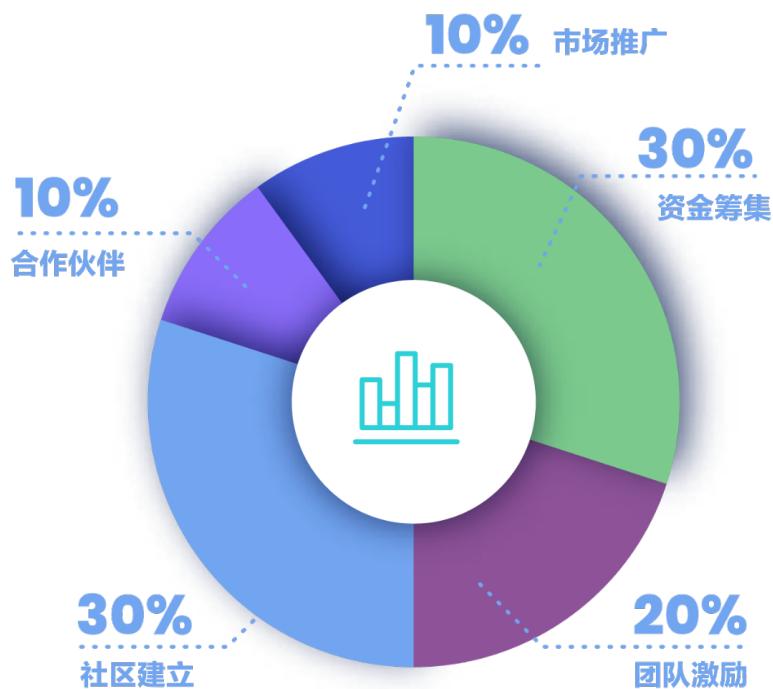


# OATH 代币机制

OATH 的代币主要用于支付法官仲裁费用，矿工节点的记账费用和社区维护管理费用。法官将通过仲裁案件获，审核法官身份，邀请更多法官，维护管理社区等取得代币回报，同时更高的信用等级将激励法官获得更高的代币奖励。矿工节点则将负责存储 OATH 的区块链数据，和负责运行 OATH 的外部服务等来获取代币。

每个案件的仲裁费用其中的5%将作为矿工的记账费用，0-5%将作为平台管理运营费用，随着案件的增多而变化，剩余的代币将按照法官案件奖励公式分配到所有做出正确选择的法官。

## 代币发行计划



OATH 将发行 10,000,000,000 个基于ERC-20标准协议的代币 (OATH Token, OST) ，用于 OATH 平台内部所有的业务。用户可以通过交易所购买，充当矿工节点，或成为法官仲裁案件，帮助维护管理社区等行为来获得代币。

OATH 将代币划分为：

- 30%** : 筹集资金
- 20%** : 团队招募, 团队激励, 等
- 30%** : 社区运营, 法官招募, 法官激励, 等
- 10%** : 市场推广, 等
- 10%** : 合作伙伴, 早期合作伙伴激励, 等

通过筹集得的资金将主要用于以下用途：

**- 技术开发** : OATH 平台依赖了复杂的算法系统和区块链技术, 同时支持多种客户端, 让用户有更便捷的使用体验。需要大量的人力来开发维护整个生态系统。使项目按计划, 高质量的完成

**- 团队建设** : OATH 团队将包含不同专业的大量顶级人才, 技术开发, 产品设计, 法律业务, 商务拓展等等, 所以良好的团队建设可以使得项目进展更迅速, 更顺利的完成项目计划。

**- 业务支持** : 由于 OATH 平台的特殊性, OATH 将联合法律法务机构共同协作一起推进整体项目, 并且以确保项目能更公平公正, 所以需要大量的法律方面的建议和支持

**- 市场推广** : OATH 平台将有效的提高智能合约的可靠性, 我们将把这个概念向大量的智能合约用户进行宣传和推广。使得 OATH 成为智能合约担保仲裁的行业标准。



# OATHS 项目计划





# OATH 团队



## 徐寅

**Founder & CEO**

毕业于美国威斯康星州立大学计算机系，毕业后就职于美国最大的健康医疗研究中心之一的 Marshfield Clinic Research Foundation, 参与研发多个医疗项目，参与发表健康大数据等论文。独立开发的心脏检测软件获2012年美国健康服务部门（HHS）举办的健康移动软件大赛全美第一名。

后加入硅谷科技公司 Trip.com 担任 Tech Lead，主导开发的App多次被Apple评为最优秀软件，获Google最佳开发者和编辑推荐奖，成为Google Store中数百万App里仅4个同时拥有两个奖项的旅游软件之一。对互联网技术，区块链，创业，团队管理等都有极高热情和经验。多年前开始关注区块链，关注以太坊，智能合约，Dapp，IPFS，EOS等区块链核心技术。



# OATH 团队

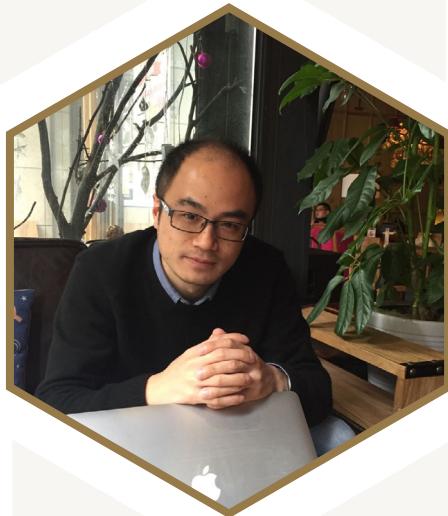


## 张博宁

**Co-founder**

2008年毕业于北京大学信息科学学院电子系，后获得中科院大学计算机硕士学位，2014年放弃博士学位投身于创业大潮。曾任职北京博扬德科技有限公司技术合伙人，爱币网（ex-btc.com加密货币交易所）安全顾问及合伙人，绵眠（上海）智能科技有限公司CTO职位，2013年起的资深区块链研究者，中国第一批加密货币交易所的创始合伙人，长期研究区块链底层技术，区块链IoT技术，和各类新型的区块链应用。对于区块链技术将来的应用与发展有充分的信心。

# OATH 团队



## 汪洪伟

**Co-founder & Head of Engineering**

2007年毕业于清华大学工程物理系。毕业后参与开发了国内最早的微博网站之一——叽歪网，并在后期领导参与了中国移动139.com项目。2009年加入FreeWheel（飞维美地）北京担任高级工程师，后于2011年加入谷歌上海并在2012年转入硅谷Google美国总部。在Google美国总部期间参与开发了Google Keep, News&Weather, YouTube, Android Auto等多个热门项目。热爱新兴技术研究和探讨，专注于系统构架，数据分析，分布式系统，计算机算法，区块链底层技术等。

# OATH 团队



## JENNY VATRENKO

**Co-founder & COO - US**

Jenny毕业于华盛顿特区乔治敦大学获得法学博士学位，和纽约市Baruch大学活动和工商管理学位。她曾是区块链基金和易资本的创始成员之一，顾问过多个优质区块链项目，为其美国和亚洲等地的商务和战略提供了巨大的帮助。在此之前，Jenny曾是一名诉讼律师，为美国最著名的诉讼事务所之一的Boies Schiller Flexner的工作6年。经手过大量巨额的商业诉讼案件，包含了“Arizona Iced Tea company”，“Bill Ackman’s pyramid scheme allegations against Herbalife”，和“Sony 影视黑客攻击案”。她的经验涉及到起诉，上庭辩护，跨州诉讼和联邦法院诉讼，和纠纷仲裁。她曾在纽约布鲁克林区认知地区助理检察官。

# OATH TEAM



## MICHAEL WURZINGER

**Community Manger**

Michael曾为西门子软件自动化的上海和孟买公司负责市场活动；其后，他于梅赛德斯奔驰最大的位于德国城市辛德芬根的生产中心，接受过为期3年的商务管理训练，并于2015年成功创办了一家家具领域的贸易公司；2016年，他于康斯坦茨大学应用科学的本科学习，攻读亚洲文化研究管理学位，并能熟练使用德语、英语、西班牙语、意大利语和普通话。

2017年加入区块链领域，现已在上海快速积累了区块链领域内良好的名声和人脉关系。作为交通大学的原访问学者，他于2018年回到上海，一边继续提升普通话，一边开始创建当地的社区，如今社区已发展到超过700位成员。他成功为NEM, EOS, AION, Lympo举办了多项活动，并在为AION举办活动时成为他们的官方代表。他对区块链技术的激情和对公共演讲、社区建立的热情，使他加入了Oath，负责 Oath 社区管理及商业战略。

# OATH 团队



## 辅容

### **Head of Quantitative Modeling**

毕业于英国牛津大学数学专业，主修数学建模方向，毕业之后在世界500强保险集团，负责风控模型。后从事风险投资工作，就职于一家美元基金，参与多个TMT项目的投资，2013年开始关注区块链，大数据方向。2015年和合伙人创立物联网公司Mirahome，负责公司整体运营及融资，公司获得数千万投资。

# OATH 团队



## 周丹瑶

**Head of Design**

本科毕业于北京林业大学，后获得美国伊利诺伊大学香槟分校硕士学位。平面/UI/UX 设计师，致力于跨行业设计与创新工作。曾就职于芝加哥 Terry Gruen 设计事务所、深圳城市规划设计研究院、好处Meetbest，涉及领域包括互联网产品UI设计、视觉设计、平面设计、插画设计、城市规划大数据可视化设计等。

参与多个线上产品UI/UX设计和各类平面封面宣传册设计。多次获得国际奖项，包括虹桥机场改建概念设计提名奖、美国能源部2013年国际太阳能十项全能优胜奖、澳大利亚墨尔本“Low Carbon Transit City”战略设计大赛荣誉奖，为中国建筑工业出版社出版的《海绵城市建设规划与管理》设计封面。

# OATH TEAM



## 黄晓玉

**Content Manager**

研究生毕业于纽约哥伦比亚大学，获理科硕士学位，本科毕业于佛罗里达州迈阿密大学，曾在日本东京大学交流修学。还曾在荷兰鹿特丹的世界顶尖事务所OMA实习，团队成员来自将近十个不同国家，项目复杂且规模庞大，需不断与当地政府、出资银行及各路甲方，及分领域专业公司等协调合作推进项目，经历了极强的高压环境，具有团队合作能力。也曾参与海地国家城镇改造及旅游开发项目，负责与各方的沟通推进，及旅游线路的规划设计。在纽约期间，曾在曼哈顿品牌公司the 7th art工作，参与多个哈德逊河边高层奢华公寓的品牌运营和管理工作，能够快速抓住产品本身特点，并快速开展品牌工作。随着大众对区块链技术共识的形成，她关注并致力于参与区块链、智能合约及各项新兴协议的发展，并对区块链技术和应用带来的发展和改变抱有很大的信心。

# OATH 顾问

**田甲**

**Advisor**



毕业于清华大学，获得计算机本科和硕士学位。曾就职于Baidu, 阿里巴巴，专注于分布式系统和人工智能研发。2011年开始关注区块链。Bitfinex投资人，Bitfund 首席科学家，真格基金 Venture Partner，Data Foundation 科学家，Cortex 首席科学家。区块链资深技术专家，大量优质区块链项目技术顾问，包括IOST, DDEX, CNN等。

# OATH 顾问



## 孔华威

**Advisor**

致公党员，高级工程师 中科院计算技术研究所上海分所所长 起点资本合伙人 先后就读北京大学、浙江大学物理系。曾任张江科投首席科学家、曙光信息产业集团VP等，专注超级计算和网格计算技术，以及区域创新生态研究，是科技部火炬创业导师，发起ITALK沙龙、IC咖啡等创新组织，参与投资芯原微电子、七牛云存储、敏狐科技、中晟光电、睿励科仪、黑子科技、鸢鼎信息、锘钛通信、语镜汽车、启能新材料等。2013年底关注比特币和区块链技术，担任壹比特公司技术顾问，著有“数字货币的崎岖演进”，目前受聘嘉楠耘智科学顾问。近年早期参与投资Scry.info, Ruff, INT, smartmesh, DBC等区块链项目。

# OATH 顾问

## 林吓洪

**Advisor**



菩提预测市场创始人兼CEO，区块链应用资深工程师，以太坊技术早期布道者，七年数字货币行业经验。前Edmodo移动端技术总监，前Twitter移动开发工程师，前腾讯研究院助理研究员。林吓洪在2017年成立菩提预测市场，致力于使用区块链技术构建下一代去中心化预测市场。林拥有普渡大学计算机科学硕士学位和上海交通大学密码学硕士学位，本科毕业于西安电子科技大学计算机系。

# OATH 顾问



**DAVID HONG**  
**Advisor**

David Hong是中国国际知名金杜律师事务所（King Wood and Mallesons）的子公司和易区块链（Heyi Blockchain）的创始人兼业务发展总监。他是许多科技公司的主要联络人，包括e投睿（eToro）和Coursera。他对区块链实现传统产业民主化和去中心化以及改善现有商业模式的能力感兴趣。他于2010年加入金杜律师事务所。之前，他在纽约的一家国际律师事务所和曼谷的另一家国际律师事务所工作。其实践侧重于外国直接投资，兼并和收购，技术和电信。他是一位华裔美国人，出生于中国重庆，在加州长大。他在加利福尼亚州的加州大学洛杉矶分校和克莱蒙特麦肯纳学院就读本科学位，并在华盛顿特区乔治敦大学获得法学博士学位。大卫现和他的女朋友以及五只猫住在上海。



# OATH 顾问



## 郭达峰

**Advisor**

毕业于香港中文大学计算机系，区块链技术专家，EOS超级节点之一EOSAsia创始人，EOS最早期的投资者之一。市面上最简易的建站平台 Strikingly 的联合创始人兼 CTO，成为第一家进入 YC 孵化器的华人团队。曾独立开发的 Facebook 应用，获取了超过 2 千万的用户。曾负责摩根斯坦利，高盛的交易系统研发。设计开发的系统服务于数百万用户，2018年被命名为阿里云技术MVP。

# OATH 顾问



## 张瑞

**Advisor**

能源区块链公司NAD Grid联合创始人，负责公司运营。致力于研究和解决区块链相关的法律和政策问题。曾就职于中信集团总部担任公司法务，具有丰富的法律从业经验，涉及领域包括公司并购、境外投资、争议解决、基础设施等。拥有中国大陆、美国加州、美国纽约州律师从业资格。本科毕业于北京大学法学院，后获得康奈尔大学法学硕士和哈佛大学公共政策硕士学位。

# OATH 顾问

## 周载南

**Advisor**



拥有清华大学自动化系学士学位和约翰霍普金斯大学计算机硕士学位。目前在谷歌公司总部担任软件工程师、Tech Lead，曾负责带领团队开发广告转化工具平台的数据汇报。在软件开发和风险投资领域有多年经验，先后在爱立信，微软研究院，StumbleUpon任职，并先后在启迪创投和zPark Venture(Amino Capital的前身)等领先的早期投资机构负责风险投资调研、创业者关系和尽职调查等。曾担任紫光集团的海外投资和并购顾问，并在多家硅谷创业企业担任出任技术及融资顾问。

# OATH 顾问



## 李嘉曼

**Advisor**

毕业于新加坡南洋艺术学院，视觉传达品牌专业。拥有多年品牌规划，市场营销，团队管理经验。曾创立两家品牌策划和活动策展公司，帮助企业打造新加坡品牌辐射东盟十国，主导策划并完成了多个一带一路项目，为国内外客户建立桥梁。在新加坡及其他东盟十国有丰富的人脉资源和市场推广经验。曾筹划举办丝绸之路国际电影节—东盟电影周，组织东盟十国主流媒体中国行等。承办中国东盟文化产能（电影）合作研修班，联合主办马来西亚电子商务展等。目前专注于区块链项目的品牌推广，活动策划，社区运营上。曾为”Influence Chain 影链”策划举办了新加坡的路演和品牌发布会，为”EasyChain 便捷链”策划举办新加坡的首发仪式，众多明星，区块链专家和数千区块链从业人员参与到活动中。



# 参考文献

1. Constitution of the United States of America

([https://en.wikisource.org/wiki/Constitution\\_of\\_the\\_United\\_States\\_of\\_America](https://en.wikisource.org/wiki/Constitution_of_the_United_States_of_America))

2. U.S. Courts: History of Jury Duty: History of the Jury. U.S. Courts for Western District of Missouri.

([http://www.mow.uscourts.gov/jury/history\\_of\\_jury\\_duty](http://www.mow.uscourts.gov/jury/history_of_jury_duty))