OATH

OATH Protocol

Blockchain Alternative Dispute Resolution Protocol

Oaths.io
Version 2.6.0

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 entity ("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 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.

CONTENTS

INTRODUCTION

BACKGROUND

Blockchain provides the general public with a useful mechanism for reaching consensus. It combines the world's leading technologies and theories, namely, theoretical computer science, mathematics, algorithms, cryptography, game theory, and economics. Blockchain brings to the world a promising decentralized internet, new ideas, and business opportunities.

To protect the decentralized communities and keep them running, we need a highly secure and trustable system. Smart contracts generally remove the barrier of trust between users. They reduce the intermediary costs that may exist in the transaction process. With unsupervised, self-executing "contracts," individuals can do business and collaborate without ever meeting or knowing each other. The design and concept of smart contracts applies to many different scenarios, such as e-commerce, insurance, home rental, banking, financial services, import and export, and many others. Smart contracts, however, have been neither widely accepted nor utilized due to several limitations: difficulties in contract preparation, inability to verify off-chain information, functional limitations, lack of on-chain governance and dispute resolution, and pseudonymity.

CORE ISSUES

DIFFICULTIES IN CONTRACT PREPARATION

Smart Contract is written in a computer programming language, such as Solidity, C++, et al. Few users have the requisite knowledge and experience to write a correct and secure smart contract. This creates an extremely high bar for potential smart contract users.

UNABLE TO VERIFY OFF-CHAIN INFORMATION

Smart contracts cannot effectively verify or authenticate off-chain information for real-world businesses, therefore creating loopholes for contract fraud.

FUNCTIONAL LIMITATIONS

Because a smart contract is a self-executing program written in a computer programming language, it works according to the terms and conditions originally written in the code. This limits its ability to resolve disputes not included in the codes.

LACK OF GOVERNANCE AND DISPUTE RESOLUTION

Decentralization is the key feature of a blockchain application. When a dispute arises, it is difficult for both parties to find a credible third party to resolve the dispute. In the decentralized world, it is particularly difficult for traditional courts or arbitration institutions to enforce the rules and resolve the disputes.

PSEUDONYMITY

Identity protection is one of the most prominent features of blockchain. Blockchain's identity protection, however, also enables potential manipulation of the system and even fraud. Although all blockchain transactions are public and immutable, one's identity is concealed (i.e., all transactions are not anonymous, but they are pseudonymous), and disreputable users may simply change their identity and commit fraud over and over again.

Those core issues we mentioned above are extremely important for smart contracts. We will have to resolve them, so that smart contracts can be safer and more useful.

CASES IN POINT

BLOCKCHAIN E-COMMERCE C2C

Party A: Seller of a pre-owned luxury handbag in "like new" condition
Party B: Buyer

Party B purchased a pre-owned luxury handbag from Party A on an e-commerce blockchain platform. After receiving the handbag, Party B argues that the bag is not in "like new" condition and requests to return it. Party A argues that the photos provided on the platform clearly show the condition of the bag, which matches the provided description. Party A refused to refund. Both sides hold their own views and cannot reach a resolution.

BLOCKCHAIN INSURANCE SERVICE

Party A: Blockchain health insurance service provider　　Party B: Patient

Party B signed a smart contract with a blockchain health insurance service provider. When Party B submits a claim for compensation from Party A, it is difficult for Party A to determine the truthfulness of the claim. For a decentralized service provider, it's difficult to decide whether the customer's claims are in compliance with the terms of the insurance, or whether the amount claimed is in accordance with the circumstances.

BLOCKCHAIN SHORT-TERM RENTAL

Party A: Landlord   Party B: Tenant

Party B rented a house through a blockchain ‘airbnb-alike’ platform. After the lease ended, Party A found that the TV was damaged and asked for compensation. Party B insisted that he is not responsible of the damage and refused to pay. As there is no centralized customer service, the two parties cannot effectively resolve this dispute.

BLOCKCHAIN COPYRIGHT PROTECTION

Party A: Blockchain Content Copyright Platform User

Party B: Copyright Owner

Party A registered IP on a blockchain-based copyright protection platform. The actual copyright owner, Party B, finds out that his copyright is pirated and appeals to the platform. Due to the lack of an arbitration mechanism, the merits of both parties’ claims cannot be determined easily.

BLOCKCHAIN BET OR PREDICTION

Blockchain prediction platforms have become wildly popular. People like to use the platforms to predict game results, campaign results, and even the weather. It is, however, difficult to determine the authenticity of some of the controversial results without external input.

As the above cases illustrate, a comprehensive smart contract system and a fair dispute resolution mechanism are much needed in the blockchain community.

OATH PROTOCOL

OVERVIEW

OATH is a blockchain-based alternative dispute resolution protocol. It is an infrastructure layer between chains and dApps. By using a decentralized juror community with a complete new consensus mechanism, Proof of Common sense, OATH provides a robust, fair, transparent, and extensible dispute resolution protocol.

OATH serves as a blockchain governance system that provides an effective warranty for smart contracts. If one side is dissatisfied with an outcome, resulting in a dispute, there will be a decentralized third party with no conflict of interest to resolve the dispute. The availability of a dispute resolution mechanism improves the reliability of smart contracts and provides a dependable protection mechanism for blockchain users.

OATH acts as an insurance protocol for dApp users, protecting them from undesirable counterparty behavior. Once the OATH protocol is initiated, OATH jury community will vote on the verdict to resolve the dispute. OATH protocol will greatly improve users' credibility and ensure that all contracts are guaranteed by an objective system and that, in case of a dispute, the parties have an unbiased, objective jury handling it.

OATH can also provide verification of real-world information, which is presently a big issue for blockchain. As a standard protocol, any dApp that utilizes OATH may request any kind of real-world information from our jury community, our jurors will provide information, and the rest of the jury community will vote to verify the information's authenticity and accuracy.

PROOF OF COMMON SENSE

OATH Protocol introduces a new consensus mechanism, Proof of common sense. It is not used by nodes to confirm the on-chain data. Instead, it is a consensus mechanism that is used within the OATH jury community.

OATH jurors only need to rely on their common sense to decide cases based on contract terms, evidence, and testimony. They do not need to be experts in any field or area. As blockchain users, they have sufficient knowledge to evaluate the evidence and determine the case outcome.

OATH jury is a community of regular blockchain supporters and dApp users. Not only will they help regulate the chain or dApp they support, but they can also provide their knowledge and service to other ecosystems. They will be rewarded for using their common sense to resolve disputes.

SOLUTIONS

OATH will provide extensions for multiple smart contract programming languages, allowing users to agree on dispute resolution solutions and default claims agreements when writing smart contracts or blockchain applications. OATH will also provide an infrastructure layer for dApps so that developers can directly integrate OATH protocol..

At the same time, OATH will also provide a smart contract construction interface that will greatly reduce barriers to using smart contracts. By providing common contract templates, OATH will improve the usability of smart contracts in a variety of scenarios. The templates will include many typical applications and scenarios, such as e-commerce, copyright protection, OTC transactions, and others. OATH protocol will be built into the template and include a dispute resolution plan, compensation agreement, and other related fields. All smart contracts written through the OATH smart contract interface are automatically secured by the OATH protocol.

The heart of the OATH protocol is our jury community. They protect the integrity of smart contracts that incorporate the OATH protocol by adjudicating any potential disputes. The OATH jury community will also serve to link news, events, and predictions between blockchains and the real world.

DISPUTE RESOLUTION MECHANISM

In the Anglo-American common law legal system, the jury operates with distinct blockchain characteristics. The jury is usually comprised of 12 jurors (each country's particular details vary slightly), randomly selected from the general adult population. At trial, the judge presides over the proceedings and resolves questions of law and procedural issues. The jury is tasked with the responsibility of resolving issues of fact at the judge's direction based on presented evidence and, based on the facts, deciding the outcome of the case.

After the closing arguments in court, the jury has the opportunity to privately deliberate and discuss the evidence presented in court. According to the judge's instructions relating to the law, the jury then decides, based on the evidence presented in court, which side prevails and returns a verdict.

The jury pool is comprised of citizens who are randomly selected from the general population, without any additional requirements of knowledge or skill. Jurors use their common sense and understanding to evaluate the arguments and evidence presented by the parties and render a verdict. Random selection results in a diverse jury composition, and the jury's diverse backgrounds and experiences ensure that the facts are considered from different viewpoints, resulting in a fair verdict. At the same time, the randomly selected jury fairly represents the general population, and the verdict based on their consensus fairly represents the consensus and understanding that the general population would reach based on the same evidence.

The jury system aligns with the decentralization of the blockchain democratic idea. All community members share the consensus that underlies the verdict, and the decisions are made by randomly selected representatives of the community.

The OATH dispute resolution protocol, therefore, is modeled on the common-law jury system and utilizes blockchain, cryptographic algorithms, random algorithms associated with categories and attributes, credit level, and case-tracking technology. OATH jurors, from different backgrounds and variant professions, guarantee to provide resolution of contract disputes by contents, evidence, testimonies and debates.

Blockchain technology will ensure the authentication of smart contracts agreements and immutability of the evidence provided by both parties.

Identities of the OATH jurors are kept strictly confidential and encrypted to make sure that their decisions are objective and free from external influence. Jurors will provide information relating to their relevant categories like age, gender, nationality, occupation, and educational level. OATH's categorized random algorithm then randomly selects jurors based on those categories. OATH will also assign a credit level to jurors to assess and reward the jurors' behavior. Jurors will get higher ratings for correctly voting for the prevailing party. On the other hand, serial wrong judgments will reduce jurors' ratings. Higher credit level results in higher awards and better odds of being selected for disputes.

OATH will establish relationship attributes for jurors to reduce the probability of joint participation in cases. This means that the same group of jurors is unlikely to be selected to resolve consecutive disputes, preventing the jurors from colluding on their votes.

The OATH platform allows the contracting parties to control the process by allowing them to set parameters for the dispute resolution process, such as the number and categories of jurors and the number of votes necessary to prevail. The verdict will be transparent, and the jurors' votes and reasons of voting will be made public once the case is closed. The decisions are appealable. The case details and dispute resolution result will be encrypted and saved on blockchain. Cases are classified and indexed as well for future reference, subject to the privacy policy.

OATH protocol aims to provide a warranty for blockchain contracts and improve their reliability, preventing the blockchain and smart contracts from being plagued by unresolved disputes. Along with the blockchain development, the OATH protocol will launch additional services for blockchain security and governance built on the principles of decentralization, justice, reliability, and efficiency.

ADVANTAGES

BLOCKCHAIN SECURITY

A fair, robust, transparent, and extensible blockchain governance protocol can greatly improve the reliability of dApps and blockchain.

QUICK AND EFFICIENT

In the event of a dispute, OATH dispute resolution cases can be generated automatically if signed and confirmed by any party, with no additional process required. Both parties will then have five days to provide relevant evidence, and the jury will have two days to review and decide the case. In most cases, it only takes 7 days to render the verdict.

JUSTICE AND FAIRNESS

OATH takes advantage of the transparency and reliability of the blockchain to make sure that the contents of each case cannot be modified or deleted. It also helps keep the jurors' identities are kept in strict confidence to preserve objectivity and prevent external influence. In addition, OATH algorithms ensure that jurors selected for each case are from diverse backgrounds.

OATH provides several options for the contracting parties to set the criteria of the dispute resolution process. For example:

Number of jurors (odd number, from 11 to 101)
Percentage of votes needed to prevail (51% - 100%)
Categories of jurors required (e.g., gender, age, nationality, language, occupation, education background, credit level, etc.)

During the voting process, neither the jury nor the parties can see the votes. After the verdict has been rendered, the votes and jurors' reasons therefor will be released publicly. Any party may appeal the result. The appealed-from outcome will not be disclosed to make sure that the new jurors are not biased. The results of the appeal will also be included in the credit level evaluation system for jurors.

MANAGEABLE COST

Users will deposit OATH tokens to facilitate the dispute resolution plan in their smart contract, which will serve as the arbitration fee for disputed cases. If the contract is successfully executed, the deposit will be returned to both parties without any additional cost. In the event of a dispute, the arbitration fee will be awarded to the jurors who correctly choose the prevailing party.

To have enough jurors willing to provide their time and effort to resolve cases, once the case is initiated, OATH will notify its jurors about key details of the case, such as arbitration fees, number of jurors required, and so on. Once they receive the notification, the jurors may decide whether they want to participate in the the case. If not enough jurors accept the case, OATH will reject the resolution plan and require the parties to change the plan details to incentivize juror participation, for example, either by increasing award to jurors or reducing the number of jurors required. This allows the parties to control and manage the cost of resolving their dispute.

EFFECTIVE EXECUTION

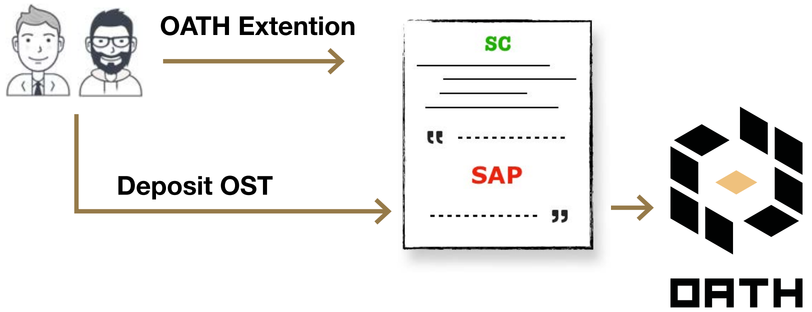
When constructing a smart contract, both parties may set a default compensation plan in advance. In the event of a dispute, once the results are confirmed by both parties (or neither party objects), OATH will automatically send the result back to the smart contract, and it will automatically execute based on the the rules originally defined by both parties.

TRACKABLE CASES

OATH will encrypt the contents of smart contract disputes and store them in the OATH blockchain. This will create an immutable case record and increase the security of smart contracts, allowing jurors and other interested parties to review the previously decided case verdicts at any time.

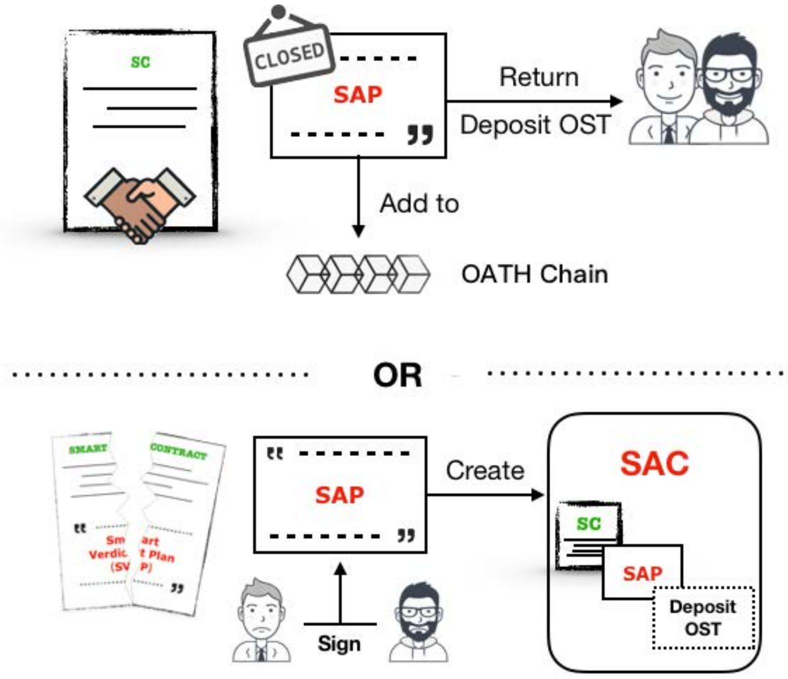
USER FLOW

01



OATH works as a smart contract extension and protocol. Through OATH, both parties can add the Smart Arbitration Plan (SAP) and set dispute resolution parameters to their smart contract at the time of its creation. SAP will require a deposit of a set amount of OATH tokens (OATH) to resolve potential disputes.

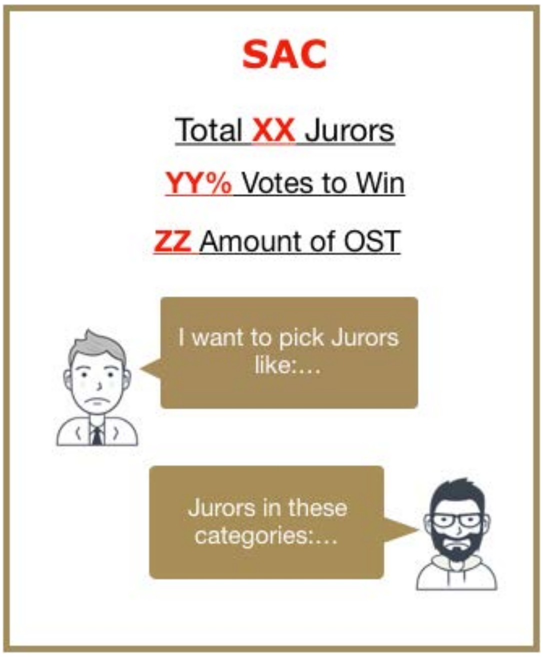
02



Once the smart contract is deployed, OATH tracks the contract progress. In the event that each party is satisfied with the result, the case is closed and the SAP returns the deposited OATH. The SAP information is then encrypted and placed on the OATH chain.

03

If either party initiates a dispute, the SAP gets converted into a Smart Arbitration Case (SAC) and the deposit into an award fee.

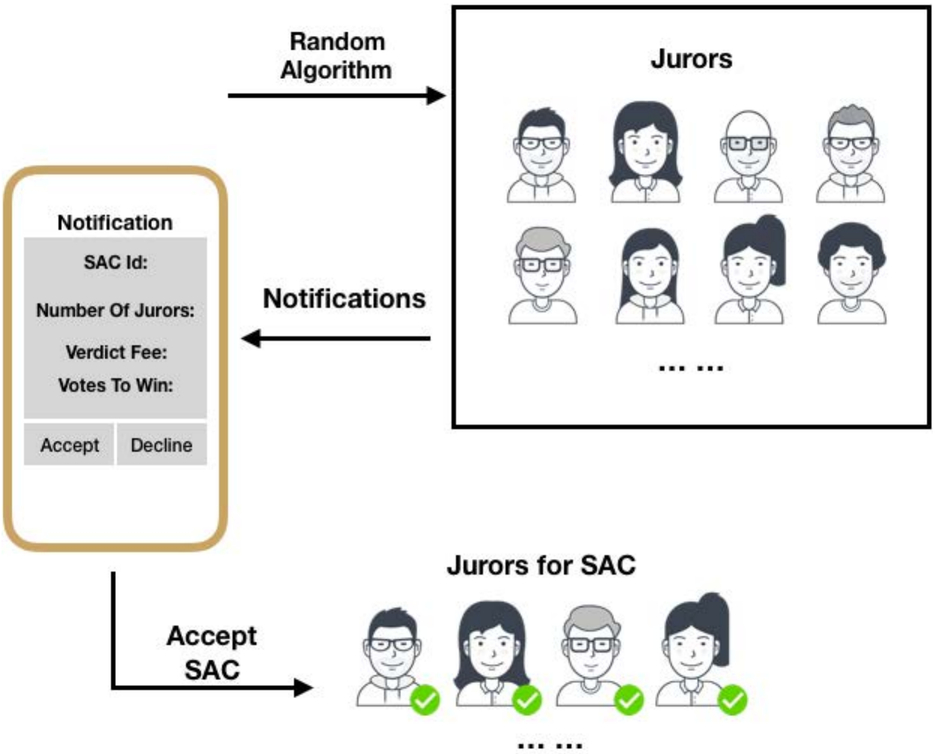

SAC
Total XX Jurors
YY% Votes to Win
ZZ Amount of OST
I want to pick Jurors like:...
Jurors in these categories:...

After that, both parties may set the following criteria for the dispute resolution process:

Number of jurors (odd number, from 11 to 101)
Percentage of votes needed to prevail (51% - 100%)
Resolution fees (by default, amount of OATH deposited into SAP)
Categories of jurors required (e.g., gender, age, nationality, language, occupation, education background, credit level, etc.)

All these settings will be encrypted and saved on the OATH chain.

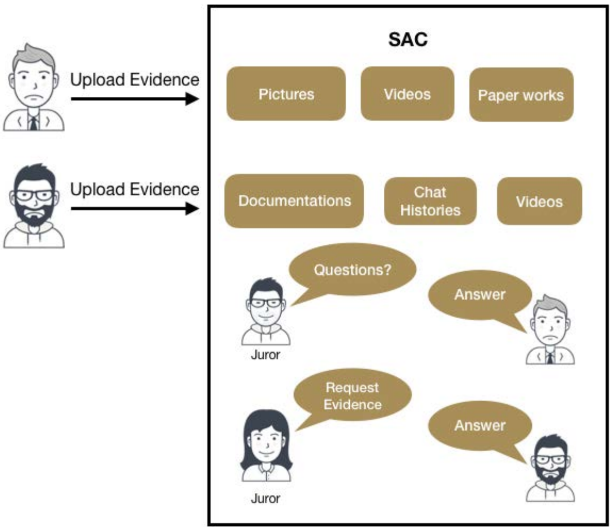
04



OATH chooses the jurors using the Categorizing Random Algorithm based on their categories and attributes within SAC settings. Two thirds of the jurors will fit the categories set by the counterparties (One third each, and if the number of jurors in full compliance is insufficient, the rest shall be filled by those partially qualified). The remaining third will be randomly selected through the OATH algorithm, excluding the categories specified by both parties.

OATH will identify twice the required number of jurors and notify them of the basic SAC details, such as the total number in jurors, percentage of votes needed to prevail, award fees, and so on. Juror candidates may decide whether to accept the case on the based on the provided information. The jury is filled on a first-come-first-employed basis, i.e., after the three major category groups (both parties and the OATH platform) have enough jurors, no more jurors will be accepted to the jury. If there is an insufficient number of jurors willing to take the case, both parties can modify the SAC to attract more candidates, e.g., by increasing the award fees or lowering the total number of jurors required.

05

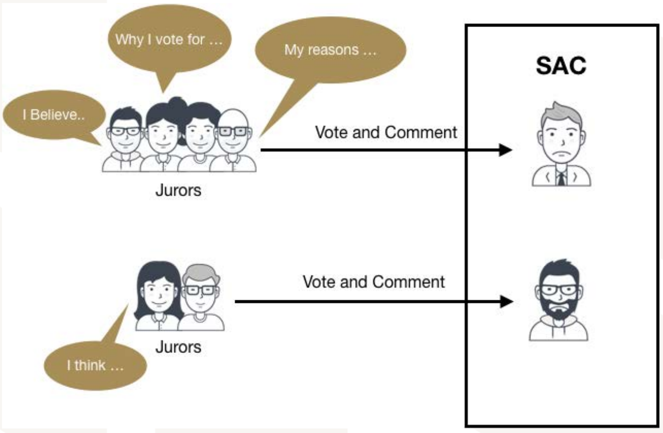


The counter-parties will have five days to upload their arguments and supporting documents (text, pictures, videos, etc.). During this period, either side may apply for an extension, paying an additional deposit in proportion to the extended days. For example, a five-day extension requires an extra 100% deposit of OATH Token.

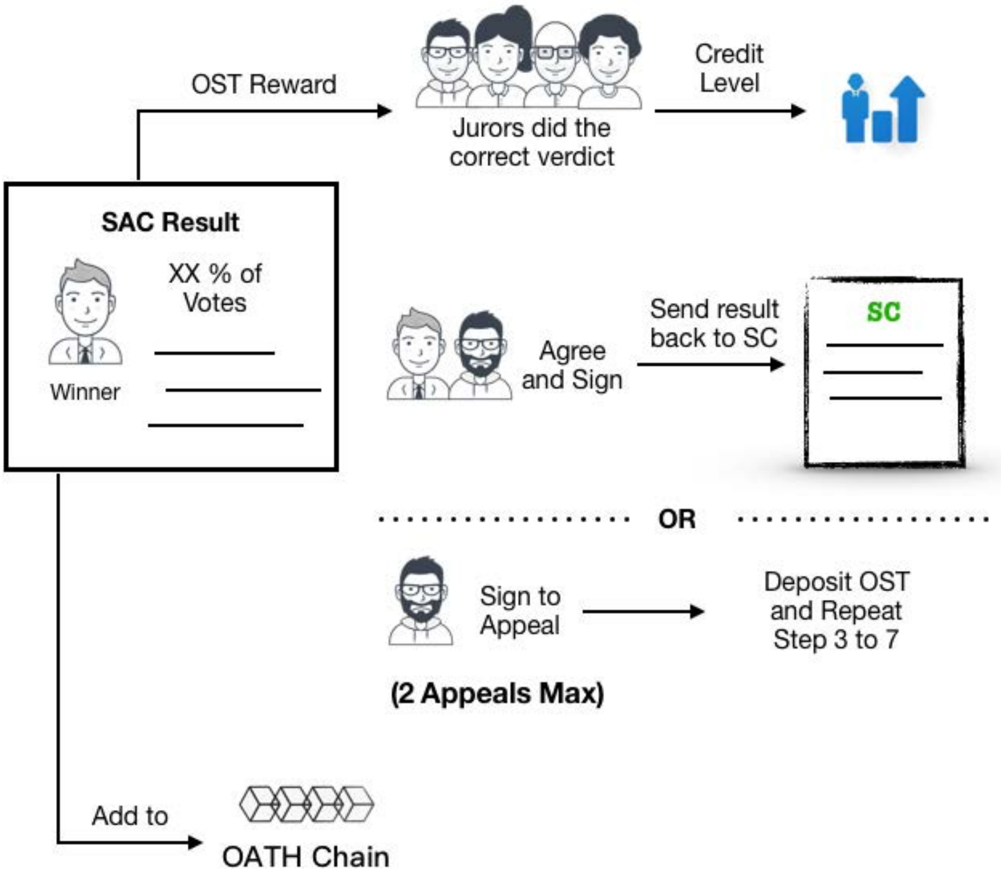
Jurors can comment on the provided materials and ask follow-up questions or request additional evidence. To incentivize participants to address critical points and participate in the discussion, community will reward their interactions by awarding token bonuses and credit scores. Jurors' identities are concealed to ensure that they remain objective and free from external influence throughout the process.

06

Once the evidence has been fully submitted, jurors will have three days to vote and provide rationale for their votes. Both parties and jurors may access the votes and written opinions only after the case is closed, and certain information (like jurors' identities) will remain confidential. Jurors who correctly identify the prevailing side will be awarded dispute fees as well as credit scores.



07



After the votes are collected, the case resolution result will become public. The result will include the votes, rationale for voting, prevailing party, and selected jurors' categories so that the parties and juror community may have a clear understanding of the result. Jurors who correctly identified the prevailing side will receive weighted awards according to the credit level formula. Judges are incentivized to achieve higher credit levels because as one's credit level increases, so do the awards.

Parties will have five days to either confirm or appeal the verdict. If both parties confirm the verdict or fail to appeal within that timeframe, OATH will send the result back to the smart contract, and the smart contract will execute automatically according to the result.

Either side may initiate an appeal, which requires an additional deposit to facilitate another round of dispute resolution. In case of an appeal, OATH will open a new SAC, repeating steps 3-7 above. Appealed-from case results will not be disclosed to new jurors to prevent bias. Appeal fees are higher, and appellate juries will be comprises of jurors with higher credit levels so that the most experienced judges are invited to decide the case on appeal. Each SAC is programmed to accept up to two appeals, and the final appeal result will be automatically returned to the smart contract.

USE CASES

OATH offers dispute resolution services for a wide range of commercial contracts covering a variety of subject matters. For instance, OATH can effectively settle disputes on e-commerce platforms, including B2C and C2C. We also help secure cryptocurrency and blockchain transactions that may present unequal trading risks. Oath's use cases include - but are not limited - to the following dispute resolution examples:

BLOCKCHAIN E-COMMERCE DISPUTES

Party A: Seller of a pre-owned luxury handbag in "like new" condition
Party B: Buyer

Party B purchased a pre-owned luxury handbag from Party A on an e-commerce blockchain platform. After receiving the handbag, Party B argues that the bag is not in "like new" condition and requests to return it. Party A argues that the photos provided on the platform clearly show the condition of the bag, which matches the provided description. Party A refused to refund.

The platform incorporates the Oath Protocol, and the dispute resolution agreement contains the following conditions:

The dispute is decided by 21 jurors, no category requirement, with prevailing ratio set at 60%;
If Party A prevails, the payment is automatically released to Party A;
If Party B prevails, the payment is automatically refunded to Party B once the item is returned to Party A.

Once Party B initiates the dispute, an SAC is created automatically. Party A uploads relevant photos, communication history with Party B, as well as a statement detailing the condition of the item. Party B also uploads relevant evidence to the evidence pool.

Once the jury reviews the evidence, over 60% of the jurors side with Party A, eliminating the need for a refund. Once both parties confirm the dispute resolution result, OATH returns the result to the smart contract, which then automatically transfers the money to Party A. Jurors are allocated their award, and the case is closed.

NEWS VERIFICATION

Party A: A group interested in accurate news reporting

Early news reporting is oftentimes vague and conflicting, due to the lack of verified information and the abundance of unverified rumors from multiple channels. OATH allows Party A to crowd-verify the facts.

To generate interest, Party A initiates an SAC and deposits OATH tokens to reward evidence-collection and verification. OATH users submit the facts and information they are aware of, and other users vote to confirm the veracity of the submitted information.

BLOCKCHAIN INSURANCE

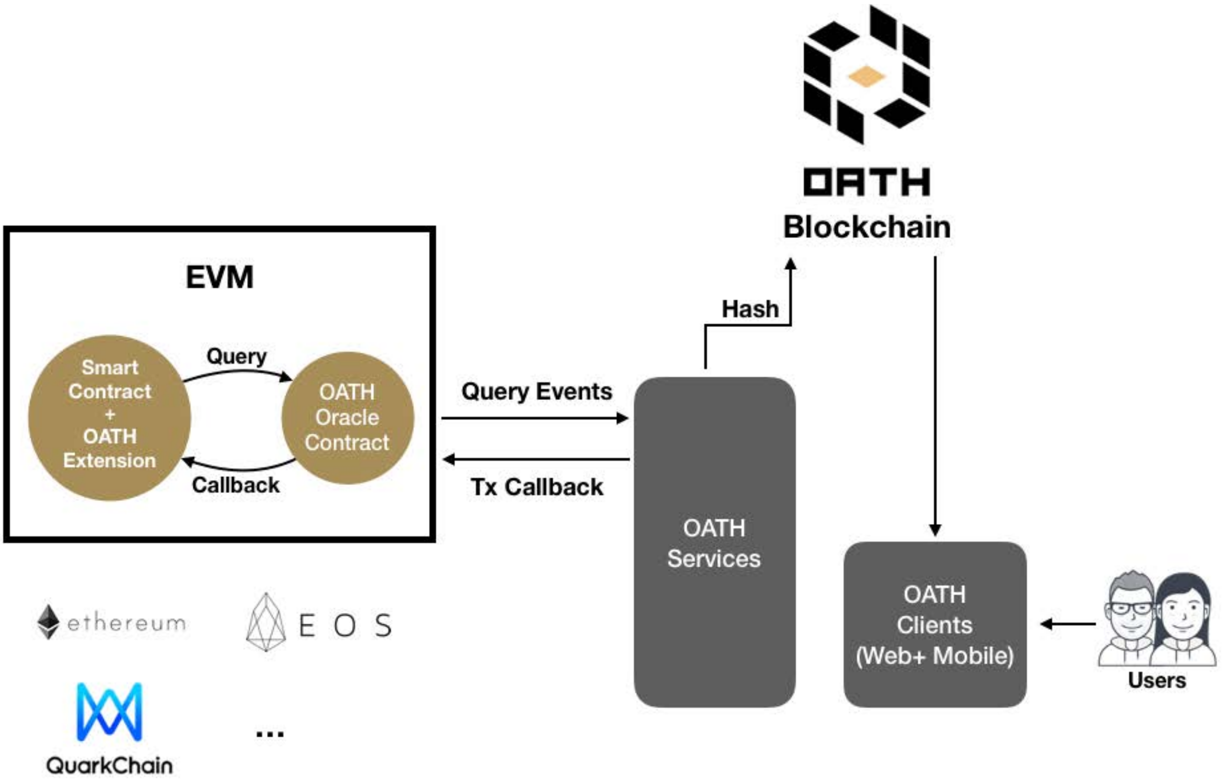
Party A: Blockchain health insurance company
Party B: Insured individual

Blockchain technology facilitates innovative insurance models, and OATH works really well with those models, providing a fair and efficient decentralized claims-verification service.

Party A and Party B signed a smart insurance contract that uses OATH as a service provider for coverage determination. To obtain insurance payment, Party B, the insured, initiates an SAC for the insurance claim. Party B needs to upload all relevant evidence to support the claim, such as pictures, medical appointment confirmation, medical billing statement and diagnosis, and so on. The smart insurance contract contents are automatically added to the SAC evidence pool. Based on the contents of the contract and provided evidence, the jurors will vote to decide whether the insured's claim is covered and he or she is entitled to the payment.

TECHNICAL ARCHITECTURE

ARCHITECTURE



In blockchain, smart contracts are executed on a closed environment virtual machine, which is an isolated system that has no interaction with external environment. This means that smart contracts are unable to communicate directly with external world or obtain any outside information.

To address this issue, an Oracle may provide off-chain data to trigger the data source to execute smart contracts. The Oracle may receive queries from the contract by monitoring specific events, and the data is returned by the callback method by the Oracle. Therefore, OATH will employ an Oracle to bridge the gap between the public chain and the OATH platform.

OATH protocol will provide smart contract extensions for mainstream public chains (including, but not limited to, Ethereum (ETH), QuarkChain (QKC), EOS.io (EOS), etc.) that contain the APIs related to OATH dispute resolution services. OATH Oracle smart contracts will also be deployed onto public chains as bridges between smart contracts and external OATH services.

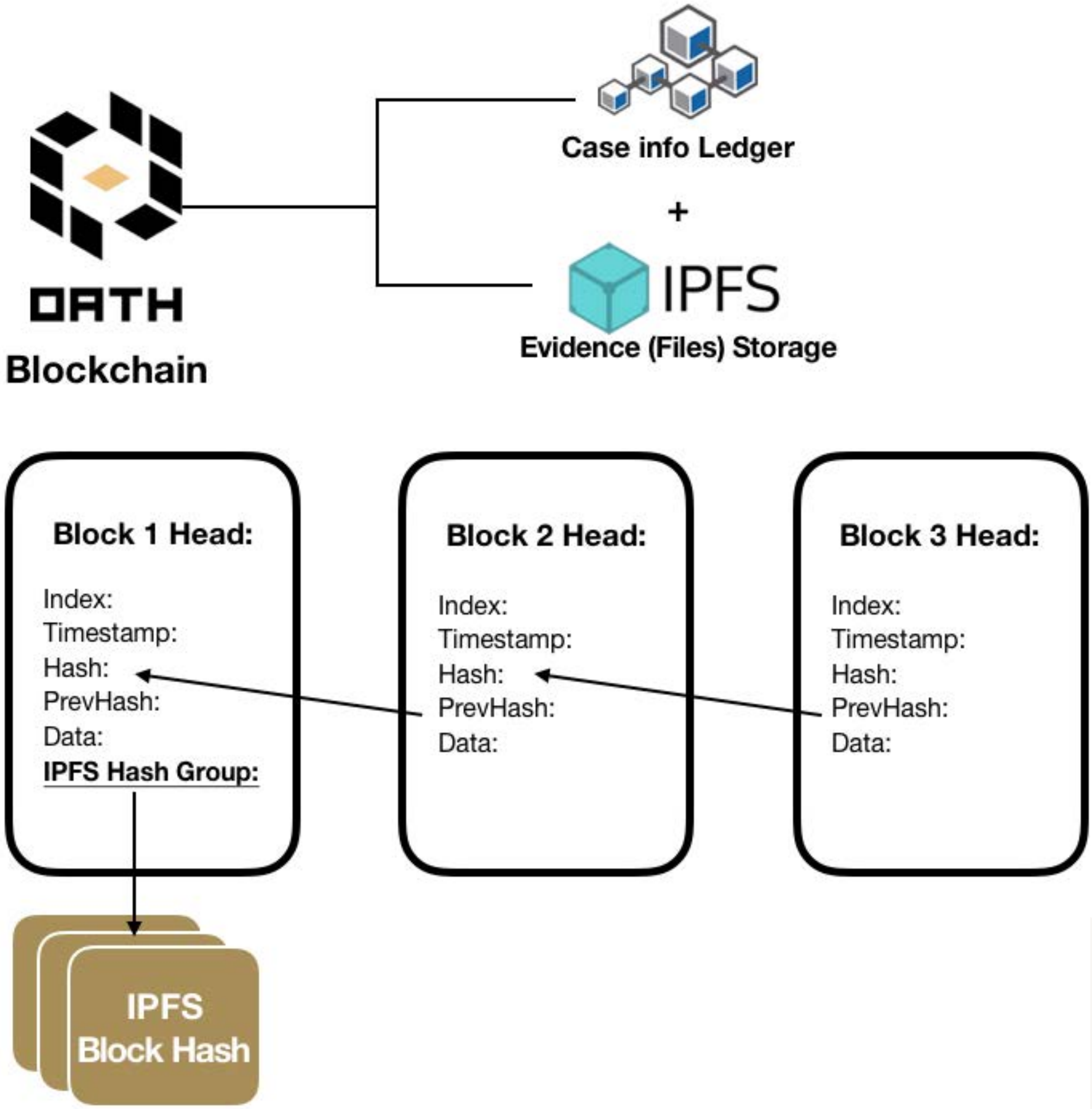
When a smart contract with built-in OATH protocol and filled APIs is successfully deployed to the public chain, it will send relevant Queries to the OATH Oracle on that chain. The OATH monitoring services will receive the relevant Query Event that the OATH Oracle sends out. OATH services will encrypt and store associated information in its blockchain (i.e., establishing resolution plans, putting on record resolution cases, etc.). If any data, such as the case result, needs to be sent back, the data will be transmitted via external services to the OATH Oracle, which will then send the data to the relevant smart contract in API callbacks. To ensure the information's reliability and security, OATH provides trustworthy techniques for proofs based on TLS Notary. TLS Notary is primarily in accordance with the secure transport layer protocol, TLS 1.1, used to guarantee confidentiality and data integrity between two communication applications. Its advantage comes from its independence from the application protocol, and higher-level protocols can be transparently distributed on the TLS protocol.

TLS consists of three basic phases:

Key algorithms supported by peer negotiation;
Public key exchange based on private key encryption and authentication based on PKI certificates; and
Confidential data transmission based on public key encryption.

Throughout the transmission, the TLS master key can be divided into three parts: the server, the auditee, and the auditor. During the process, data sources from the OATH node serve as the server side, OATH services serve as the auditee, and a specially-designed, open-source service deployed on the cloud platform serves as the auditor. Everyone can review and verify the data provided by OATH in the past through this auditor service to ensure the integrity and security of the data.

OATH BLOCKCHAIN



The OATH chain contains one case ledger and one IPFS for file storage.

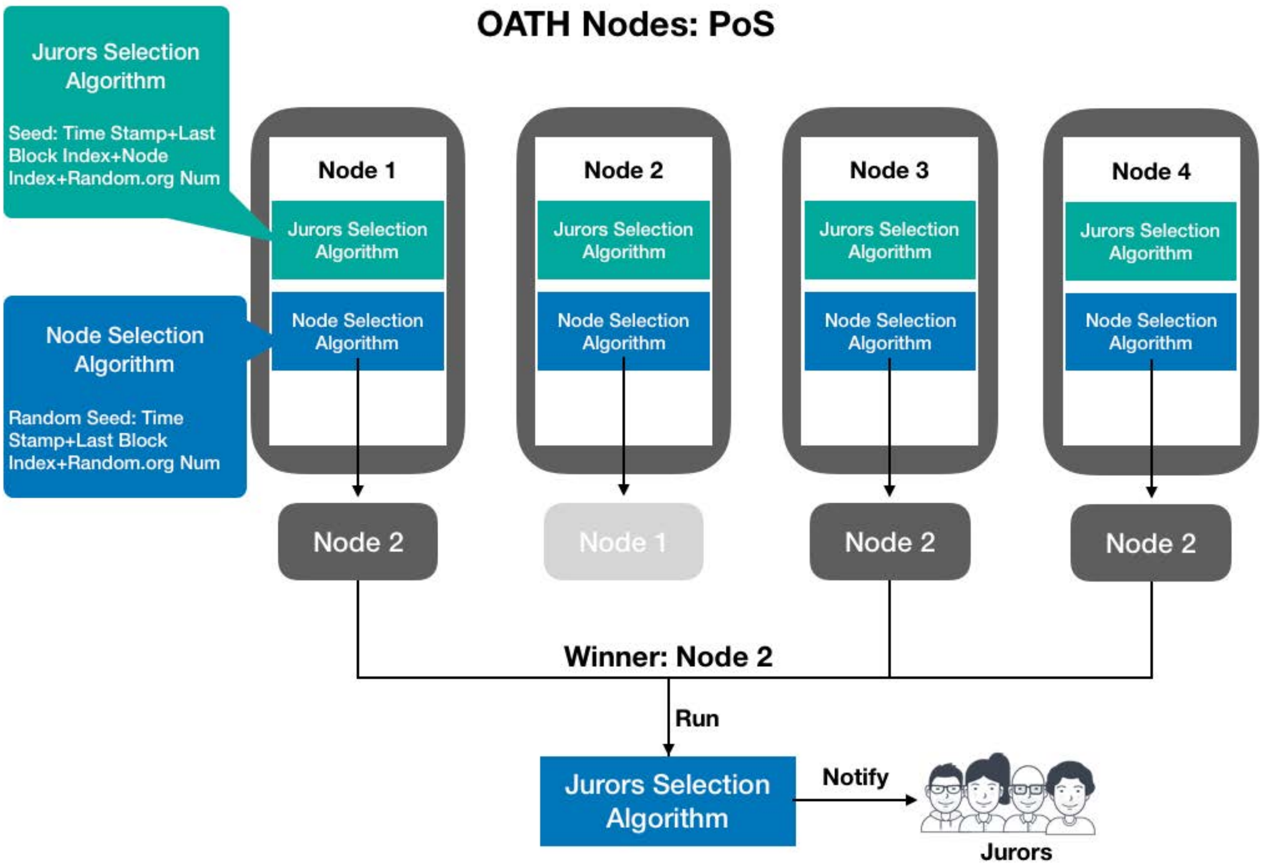
The case ledger contains all case information, such as contracts, verdicts, voting reasons, selected jurors, etc. OATH will also have an IPFS to store case-related evidence files.

The IPFS (InterPlanetary File System) is a network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. It replaces traditional domain names with content addresses so that users don't have to consider names and paths of file storage. Placing a file on the IPFS chain yields a unique hash value calculated based on its content. The hash value directly reflects the contents of the file. Even a one-bit change can result in a completely different hash value. When IPFS is requested to calculate the hash value of a file, it will use a distributed hash table to find the node where the file is located, then retrieve the file and verify the data contained therein. IPFS is a general-purposed infrastructure with few storage limitations, in which large files are divided into small sections that can be downloaded from multiple nodes at the same time.

IPFS is a flexible, fine-grained, distributed network that is well suited to the requirements of content storage and distribution. If evidence is contained in the case information ledger, there will be additional IPFS Hash Group data that contains IPFS Hash Key for all related evidence files. An encryption algorithm will generate the private key for the IPFS-stored file, whose contents will not be disclosed to ensure the security and confidentiality. The case information will be formed by several linked blocks, such as:

SAP block, which contains encrypted contract contents, contract currency, billing addresses of both parties, etc.
SAC block, which contains its own hash value, information about the jurors who decided the case, IPFS Hash Group of the case evidence, etc.
SAC verdict block, which contains the hash value of the SAC block, encrypted voting results, voting processes, etc.

NODES


OATH Nodes: PoS
Jurors Selection Algorithm
Seed: Time Stamp+Last Block Index+Node Index+Random.org Num
Node Selection Algorithm
Random Seed: Time Stamp+Last Block Index+Random.org Num
Node 1
Node 2
Node 3
Node 4
Jurors Selection Algorithm
Node Selection Algorithm
Node 2
Node 1
Node 2
Node 2
Winner: Node 2
Run
Jurors Selection Algorithm
Notify
Jurors

The OATH Chain nodes adopt the consensus mechanism of PoS. Each node is responsible for storing case information and evidence files. The nodes also run OATH's external services, such as Oracle Query Event monitoring services and juror selection algorithms.

The monitoring service on the Nodes monitors query events sent out by the OATH Oracle and conducts corresponding operations through the information contained within. All nodes will be monitoring collectively, and after receiving the Event information, the nodes will compare and confirm it with nearby nodes. Once more than half of them are confirmed, a Node will be selected by the 'PoS Node selection algorithm' to start running the relevant services.

For jurors' selection algorithm, OATH uses the categorized random algorithm, which will randomly select jurors based on certain categories. The random seed is constructed by current Timestamp with the latest block index and random numbers generated from Random.org. Adding random numbers from Random.org increases the randomness and security of the algorithm.

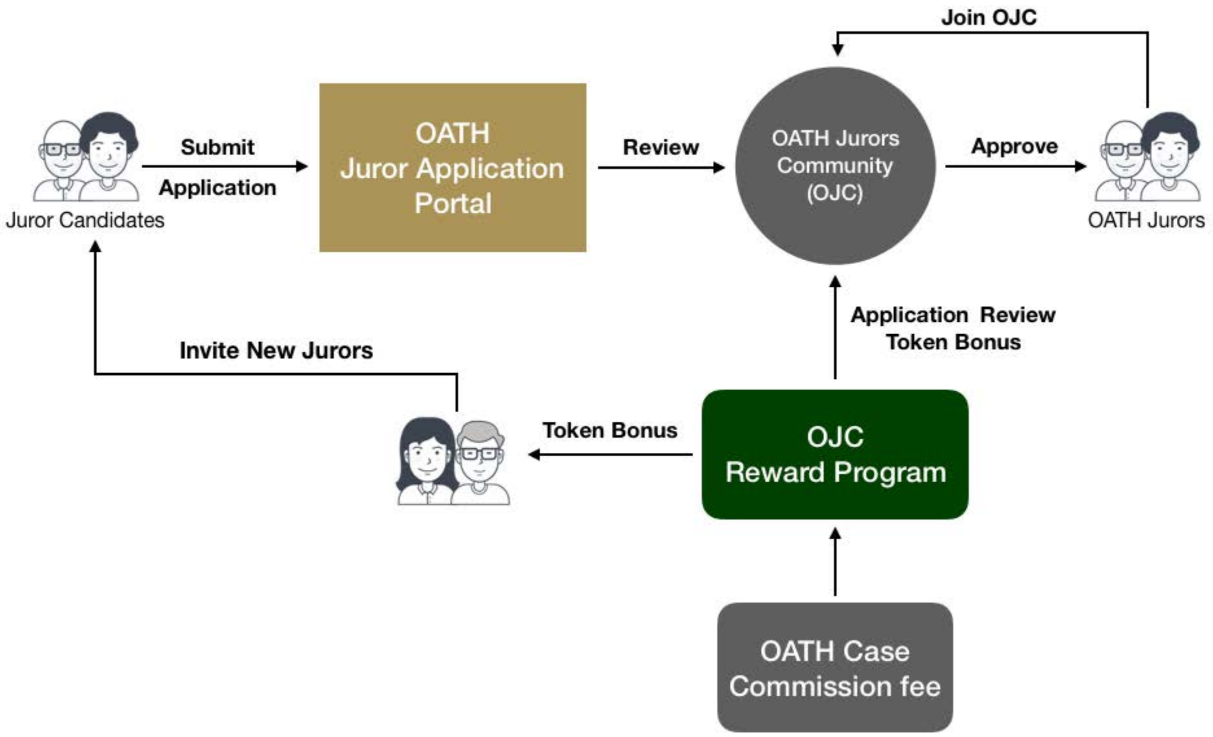
OATH will provide two user clients: a web app and a mobile app. The web app is mainly responsible for case presentation, initiation, evidence upload, voting, result presentation, etc. The mobile app will have similar functions to the web app, providing an additional convenience of push case notifications to the jurors.

JURY SYSTEM

KYC & IDENTIFICATION

Users may apply to serve as jurors on the OATH client. To do so, they will need to submit certain information, like gender, age, nationality, language, professional background, occupation, etc. For the purpose of providing fair and reasonable dispute resolution services, initially, OATH will have a Jury Community Management (JCM) team. The JCM team will examine the identities and qualifications of juror applicants and set initial credit levels according to the applicants' backgrounds. The JCM team will also run promotions to incentivize a robust juror community, e.g., bonus awards for new jurors joining the community; bonus awards for maintaining a successful track record, etc.

As the number of jurors increases, the community will conduct this process autonomously. Community jurors with high credit levels can review the backgrounds and identities of new applicants, recommend candidates, vote for approvals, and determine initial credit level through comprehensive scoring. They will be rewarded by tokens for successful approvals and when their referrals correctly decide a certain number of cases.



CATEGORIES & ATTRIBUTES

Every juror in the OATH community is assigned Categories and Attributes. Categories contain their personal information and serve as keys for classification and more scattered random screening. Attributes are designed to avoid possible collusion or fraud, and are adjusted based on the juror's case history and the platform development.

Categories include: age, gender, nationality, language, major, occupation, education, etc. Because fair resolutions require consensus of the general public, OATH will pool jurors from diverse backgrounds to decide each case. Users will provide the relevant category information in their applications. Once the information is submitted, it can be modified via a subsequent application that requires approval by the juror community.

Attributes reflect the map of dynamic relationships between jurors, tracking whether any two jurors have participated in the same case. OATH will record this collaboration relationship and prioritize jurors with no recent attributes in recent cases. This map is constantly adjusted, avoiding potential collusion and fraud that may to occur in continuous groups.

JUROR SELECTION ALGORITHM

To select jurors, OATH uses the modern version of the Fisher-Yates shuffle algorithm, presented by Richard Durstenfeld in 1964 and popularized by Donald E. Knuth in The Art of Computer Programming.

The algorithm is used to generate a random permutation of a finite sequence; in other words, the algorithm shuffles the sequence. The algorithm effectively puts all the elements into a hat; it continually determines the next element by randomly drawing an element from the hat until no elements remain. The algorithm produces an unbiased permutation: every permutation is equally likely. The modern version of the algorithm is efficient: it takes time proportional to the number of items being shuffled and shuffles them in place.

In the first step, the Fisher-Yates algorithm generates a random sequence of all jurors. In the second step, the jurors are divided into three groups (two category-specific groups and one random group) based on the conditions specified by the parties. Because the party-specified conditions might not be mutually exclusive, it is possible that the same juror fits both category-specific groups. In that case, the juror is placed into the group with fewer members or, if both groups have the same number of jurors, the juror is places in the first-matched group. If a juror does not match either party's specified categories, the juror is placed into the random group. Once all three groups are filled, the process is completed.

The complexity of the algorithm is O(N), which is proportional to the number of jurors.

```
let a := array_of_jurors
let n := a.length

struct bucket {

    data; // juror bucket array
    func; // function returns true if the given juror fits the requirement for this bucket
}

// Phase-1 Fisher-Yates shuffle
for i from n-1 down to 1 do
    j ← random integer such that 0 ≤ j ≤ i
    exchange a[j] and a[i]

// Phase-2 Bucket filling
let fulfilled := false
for i from 0 up to n-1 do
    If bucket_1.is_full() and bucket_2.is_full() and bucket_3.is_full():
        fulfilled = true
        break
    If (not bucket_1.is_full()) and bucket_1.func(a[i]):
        bucket_1.data.append(a[i])

else if (not bucket_2.is_full()) and bucket_2.func(a[i]):

        bucket_2.data.append(a[i])
    else if not bucket_3.is_full:
        bucket_3.data.append(a[i])

// Phase-3 final check
if not fulfilled:
throw exception(“No sufficient amount of jurors for this el
ection”)
```

JUROR CREDIT LEVELS

OATH introduces a Credit Level System to encourage and enforce reasonable and fair decision making by the jurors. The system has 20 levels, and jurors with higher credit levels earn more heavily weighted token awards for services performed on the platform. New jurors, after KYC verification and evaluation by a number of statistical methods, are assigned an initial credit level, from 1 to 5. Jurors may level up once they reach certain point thresholds, and jurors accumulate points through active case participation and correctly deciding case outcomes.

Jurors' credit levels and scores can be expressed as follows:

In which, L ∈ [1, 20] is the credit level, P stands for the credit score, ε (t) is the standard step function satisfying the description of the standard saving signal, and Fibo stands for the Fibonacci sequence.

the credit level numerical table is as follows:

Changes in credit scores are determined by several factors in each case of dispute resolution:

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

Credit scores are determined by the following factors:

1. Voting: Correctly deciding case outcomes (voting for the prevailing party) has the biggest impact on credit scores. Voting for the winning party earns 2 points, whereas voting for the losing party subtracts 2 points. To maintain the fairness and stability, platform will greatly decrease the credit scores of jurors who make continuous wrong choices

2. Response Time: Timeliness also affects one's score. Jurors have to render verdicts within the prescribed period. Voting within that period earns 1 point. Failure to make a decision within the prescribed period results in a null vote, which may affect the case outcome. Overtime decisions, therefore, subtract 2 points from the score, and repeat failures to render timely decisions will result in heavier penalties.

3. Appeals: Although no juror can satisfy all expectations and fit everyone's concept of justice, jurors are motivated to render objective and unbiased verdicts. The appellate review, handled by higher-leveled jurors, sufficiently reduces the potential for bias. If the appeal is denied (and the original result is upheld), prevailing jurors' votes will earn an additional 1 point, to reward them for correctly deciding the case outcome. If the original result is overturned, however, former prevailing jurors will lose 3 points, and jurors whose votes align with the appellate result will earn 2 points.

Credit Level	Points	Points to level up
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
14	986	610
15	1596	987
16	2583	1597
17	4180	2584
18	6764	4181
19	10945	6765
20	17710	

CASE

Juror Bob made the right choice in a dispute resolution case, in which he was awarded 2 points. The choice was made within the specified time, for which 1 point was awarded, 3 credit points in this resolution. Bob obtained 3 points in this case. Assume that this dispute case is appealed, and higher-leveled jurors will be selected. Although Bob has no right to participate, he will still receive an extra point if the appeal is upheld. In the end, he obtained four credit points for his involvement for the verdict.

For Example: Bob earns 2 credit points for voting for the prevailing party, and an additional point for voting within the prescribed time frame, earning a total of 3 points for participating in the dispute resolution case. If the case is appealed, and the result is upheld on appeal, Bob will receive an extra point. At the end, Bob will have earned 4 points for correctly and timely deciding the case.

Assume a juror gets Pi credit scores after each case:

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

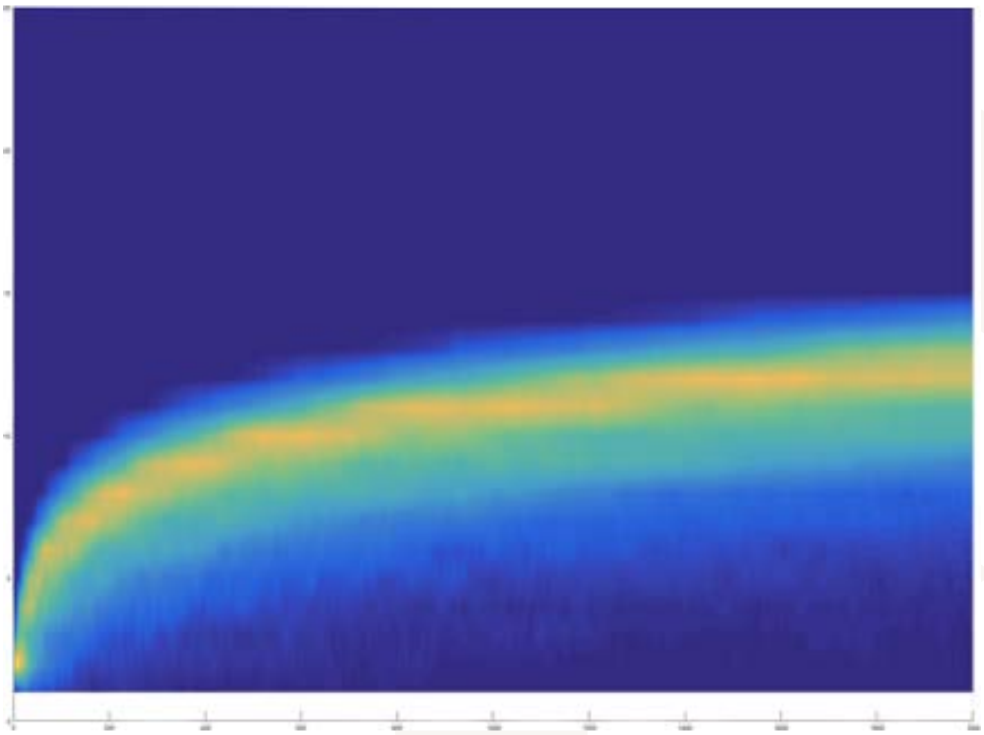
$R(r_i)$ is the credit integral function corresponding to case voting results

$T(t_i)$ is the credit integral function corresponding to case decision time

$C(c_i)$ is the credit score function corresponding to appeal results

The juror's cumulative credit score is $P_{total} = \sum P$

To improve the durability of the OATH platform, we simulated the credit level distribution of jurors after 2000 cases. Most jurors end up between levels 5 and 15, and the difficulty of upgrading to higher levels exponentially increases.



THE HIERARCHICAL DISTRIBUTION OF JURORS AFTER 2000 DISPUTE RESOLUTION CASES

REWARD MECHANISM

A juror's credit level is a reflection of that juror's professionalism and good judgment. To facilitate and maintain a healthy growth of the platform, OATH encourages jurors to obtain and maintain a high credit level, which increases their token awards. Within the OATH platform, each juror's token award is proportional to that juror's credit score. The specific distribution is as follows:

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

Fee is the total resolution payment of the dispute, S_j is the current credit score of the Jth juror,, and R_j is his/her reward.

To facilitate community growth and development, early jurors may be assigned higher credit levels and awards, and early adopters may also be involved community growth and management to ensure sustainability and operation of platform.

OATH TOKENS

OATH will issue 10 billion (10,000,000,000) ERC-20 tokens (OATH) to facilitate all transactions that take place on the OATH platform, mainly as awards for resolving disputes, mining nodes, and community maintenance and management.

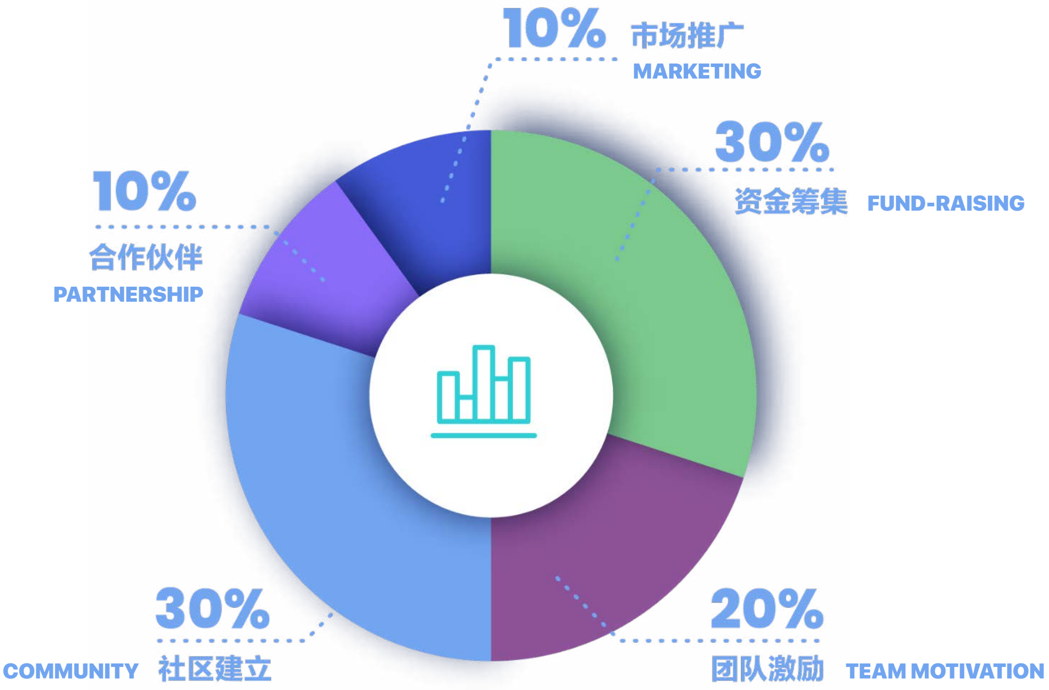
OATH can be earned by community members for acting as nodes, arbitraging contracts, or providing other community services.

Jurors will be rewarded with OATH tokens for participating in dispute resolutions. In each case, the jurors who correctly vote for the prevailing party will be rewarded according to the "Case award formula." Jurors may also get rewarded for inviting more jurors and maintaining and governing the Juror community by reviewing new juror applications, setting categories for new jurors, reviewing finished cases and providing feedbacks for jurors, and so on.

The mining nodes will get OATH tokens by providing data storage, running algorithms, and other OATH platform-related blockchain services.

To utilize the OATH protocol, users will have to pay a certain amount of OATH Token as the operating cost of the platform, which will vary with the number of outstanding cases and the liquidity of OATH tokens.

ALLOCATION



OATH tokens will be allocated as follows:

30%: Fundraising

20%: Team, recruitment, etc.

30%: Community operations, recruitment of jurors, incentives for jurors, etc.

10%: Marketing

10%: Strategic partners and advisors

Raised funds will be allocated as follows:

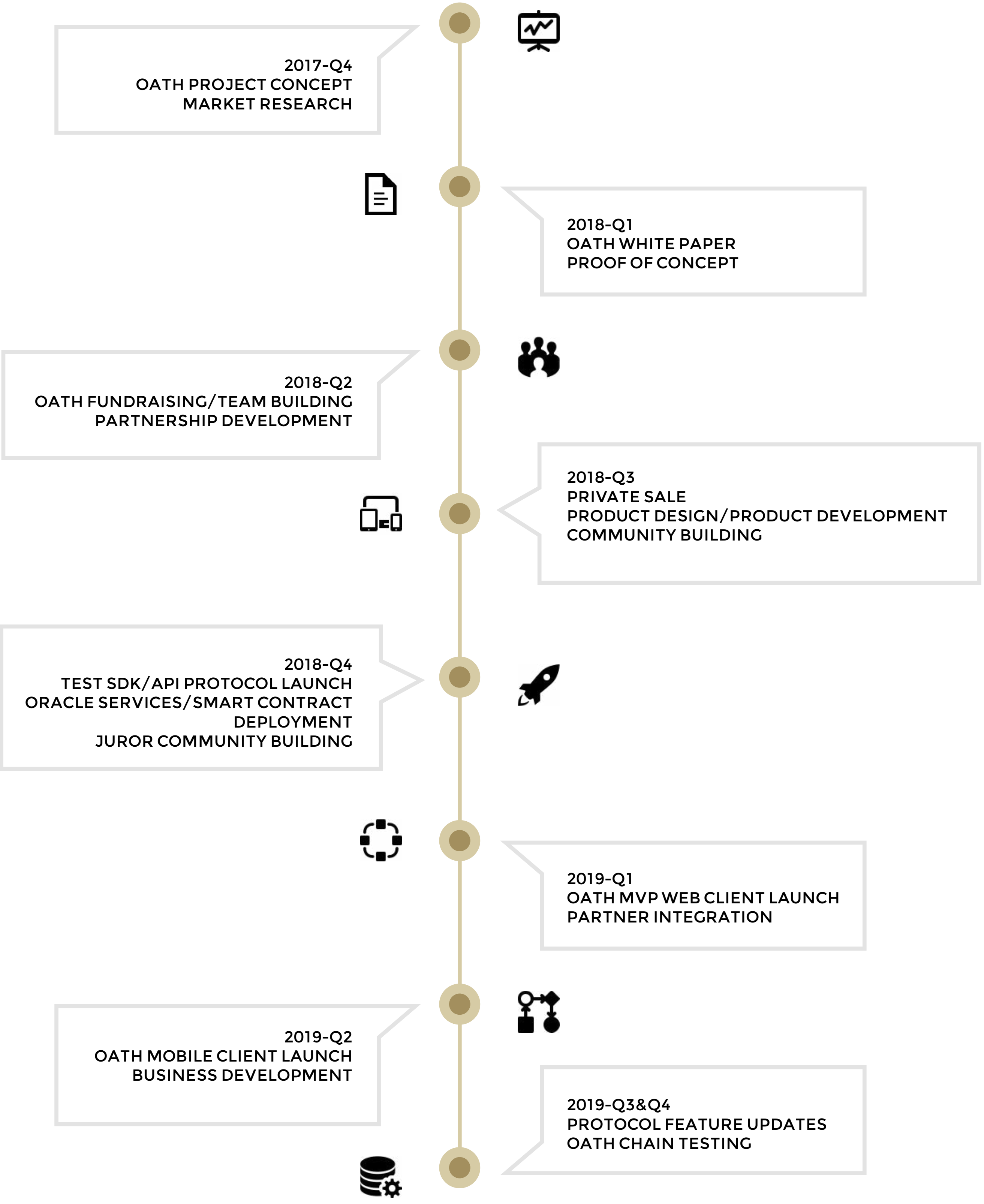
Product development: The OATH platform relies on complex systems, blockchain technology, multiple user clients, and so on. We need a solid, experienced team to develop and maintain the entire ecosystem and carry out the project of the highest quality as scheduled.

Team building: The OATH team includes professionals from different areas of expertise, such as blockchain technology development, product design, legal business, business development, marketing, community management, user growth, etc.

Business development: To provide a great product and a fair system, OATH will work with legal authorities across jurisdictions to advance the overall project. OATH will also work with major public chains and reputable dApps to advance the protocol's use in different areas.

Marketing: The OATH Protocol aims to become the standard blockchain dispute resolution protocol and effectively improve the reliability of smart contracts.

PROJECT ROADMAP



2017-Q4
OATH PROJECT CONCEPT
MARKET RESEARCH

2018-Q1
OATH WHITE PAPER
PROOF OF CONCEPT

2018-Q2
OATH FUNDRAISING/TEAM BUILDING
PARTNERSHIP DEVELOPMENT

2018-Q3
PRIVATE SALE
PRODUCT DESIGN/PRODUCT DEVELOPMENT
COMMUNITY BUILDING

2018-Q4
TEST SDK/API PROTOCOL LAUNCH
ORACLE SERVICES/SMART CONTRACT DEPLOYMENT
JUROR COMMUNITY BUILDING

2019-Q1
OATH MVP WEB CLIENT LAUNCH
PARTNER INTEGRATION

2019-Q2
OATH MOBILE CLIENT LAUNCH
BUSINESS DEVELOPMENT

2019-Q3&Q4
PROTOCOL FEATURE UPDATES
OATH CHAIN TESTING

REFERENCES

1. 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)