

Jury.online

Alexander Shevtsov

October 16, 2017
v2.4

Contents

1	Introduction	2
1.1	History	2
1.2	Problems	3
1.3	Objectives	4
1.4	Blockchain	4
2	Description	5
2.1	Overview	5
2.2	Operation	5
2.3	Use cases	7
3	Jury.online protocol	8
3.1	Requirements for participants	9
3.2	Attachments	9
3.3	Smart contract of a deal	9
3.4	Multiparty deals	10
3.5	Requirements for pools	11
3.6	Selection of judges	11
3.7	Summary of the working scheme	12
3.8	Judges' verdicts	13
3.9	Ratings	14
4	Jury.online platform	15

4.1	Operation	15
4.2	Connection of pools	15
4.3	Economy	16
4.4	Jury.online commission	17
4.5	Appeals	17
4.6	Protocol development, research	18
5	Features	18
5.1	Escrow	18
5.2	Jury market	18
5.3	Jury pools	18
5.4	Customization of dispute resolution	19
5.5	Integration	19
5.6	Security	20
5.7	Paranoid mode	20
5.8	Statistics	21
5.9	Audit	21
6	Initial coin offering	21
7	Roadmap and milestones	23
8	Epilogue	23

1 Introduction

1.1 History

Deals and contracts are an integral part of human life. Today they come in many forms as a result of human and computer interactions. However, since commodity trading markets evolved millennia ago in Mesopotamia until today trust remains paramount in business relationships and global trade.

Yet, when business relationships are challenged or fail, parties may seek justice and protection of their interests in courts arbitration and private settlements. The development of global judicial systems and legislation has

not kept pace with the progress of technological innovation, especially in newly emerging markets and technologies.

National laws are not yet corresponding to realities of the modern world, and existing legal cases have clogged the already overburdened judicial process, which has coincided with a steep rise in the cost of legal services and litigation.

Let's have a glance at the contemporary problems of dispute settlement.

1.2 Problems

Modern litigation or other kinds of dispute resolution are completely outdated and have a number of fundamental disadvantages:

- High price. Professional legal services are extremely expensive, with preliminary consultations alone costing hundreds of dollars, while attorney's fees for managing civil lawsuits account for thousands of dollars.
- Duration of proceedings. As a rule, it takes several court sessions with 1-2 months intervals to solve a case. That, of course, is too long for most disputes.
- Execution of judgement. Even if a judgement is delivered, its execution takes time and is carried out by third parties. The losing party may abscond, declare bankruptcy or otherwise escape from fulfilling its obligations.
- High entry requirements. Most often, only big cases are considered in courts, and few people are ready to start serious litigation for disputing over some everyday matters, like poor-quality product or service. The cost and complexity of proceedings do not depend too much on subject of a deal.
- Jurisdictions. State courts administer justice under the laws of a certain state which vary significantly in different countries.
- Political engagement and bias. Courts are not always independent — often they are influenced by other institutions and people.

- Complexity. Only few people can protect their own interests, for the rest trials are very complicated.
- Lack of choice. There is no way to choose specific rules to be used for dispute resolution. Usually it is the national legislation of a certain country which cannot be altered by the parties.

1.3 Objectives

Due to the problems mentioned in the subsection above, we consider current execution and regulation of deals to be completely outdated and want to change them by creating an interaction protocol for judges and parties of a deal, as well as a transparent, secure, and convenient platform for making deals using blockchain and modern cryptographic systems.

1.4 Blockchain

Blockchain technology became widespread after 2008[2]. Blockchain is ledger of information blocks with built-in fault tolerance and absence of centralized control. It can be thought of as a decentralized database with distinct rules of update. For today, blockchain is the best tool for solving problems of trust and security.

The information stored in blockchain network is open, since common database simultaneously exists on all computers that are part of the network. All changes in the blockchain are carried out stage by stage by means of transactions, each of them being open to everybody. Blockchain cannot be corrupted, since all changes to be made should satisfy the rules, and the rules are predefined by the protocol specification which is developed by community. Moreover, changing even a single unit of information requires changing the information on every computer connected to the blockchain, which is impossible.

Blockchain also involves transfer of value — cryptocurrency. The transfer of cryptocurrency has all the advantages of the blockchain: openness and unforgeability, while the transfer fee is much lower than that in banks.

Furthermore, blockchain gave rise to the technology of smart contracts, i.e. autonomous network agents capable of interacting with other network members, including people. Smart contract operation is defined by the program code stored in the blockchain and open to everyone, making it possible to realize complex interactions between network nodes. The course of such interactions is open and unchangeable.

2 Description

2.1 Overview

Jury.online enables users to make deals which, in case of dissatisfaction of any party, are considered by a panel of jurors delivering judgement in favor of one of the parties. Jury.online also gives any person with expertise in certain field an opportunity to use their experience and knowledge for paid dispute resolution.

2.2 Operation

A person willing to initiate a deal should open the website or mobile application and create a deal using one of the ready templates and specifying all important details.

The deal is then placed into the blockchain as a smart contract. After the deal is accepted by the other party, it cannot be deleted or changed by anyone, even the platform administration has no control over this smart contract. In addition, the deal is assigned with a link which leads to the website page displaying information about the deal. The initiator sends this link to the counterparty or makes it accessible to the public if they do not yet know who is going to be the counterparty. For example, a deal is intended for product or service delivery, but the initiator does not know who is going to perform it.

When creating a deal, the initiator indicates a sum they are ready to pay for the job (or want to get, if the initiator is a contractor). This sum, converted into cryptocurrency, is sent to the balance of the smart contract, i.e.

deposited. This money cannot be withdrawn until the deal is completed, regardless of whether it was successful, whether the parties were content about its execution or need to start legal proceedings. Part of the balance is allocated to resolve possible disputes, i.e. to pay court fees (it's not the only option, fees can be paid separately).

After the counterparty confirms its consent to the terms and conditions of the deal and specifies the information necessary, the deal is considered to be concluded.

After that, the parties have certain period of time to fulfill their obligations. In the event each party is satisfied with the result, the money from smart contract of the deal is transferred to the counterparty (or elsewhere, if specified by the deal), and the deal is considered to be successfully completed.

In the event one of the parties is not satisfied with the deal execution and believes that the counterparty has not fulfilled its obligations, the deal is sent for judges' consideration. Any party may initiate a dispute and send the deal to judges, but as a rule it is the party that deposited money.

When initiating a dispute, the parties have certain period of time to set forth their arguments and comments on the issue. After that, the deal is sent to judges for consideration.

Form of dispute resolution may vary, but usually the system chooses n random judges who receive anonymized information about the deal and take the decision by an absolute majority of votes.

Judges are provided by a source called a judge pool: in the simplest it's done by Jury.online, but third parties specializing in a certain sphere may also offer dispute resolution services.

The identity of judges is unknown to the parties, but their competence is. Judges have a fixed period of time to take a decision. Information about the decision of a particular judge is encrypted and unavailable to other judges.

There are other forms of judging accessible: instead of several random unknown judges the parties may agree on a specific judge they consider fair and uncorrupted.

Most deals imply performance of contractual obligations for a payment. In this case, one party has automatically fulfilled its obligations as it has trans-

ferred the payment to a smart contract, and it is the only party interested in dispute. However, we do not want to limit the range of possible deals, for example, service for service or other options, so it is possible to choose who and when is to pay for possible litigation.

2.3 Use cases

Here are several examples of using jury.online platform and protocol:

- The party is a company that needs to design a logo or write a text by certain terms of reference. The company is quite well-known and pays well, thus expecting proper quality of the works performed. The counterparty is an artist without any outstanding works who hasn't used jury.online service before. The party wants to hire the counterparty but needs guarantees that the job will be done on time.

In this case, the party is the one interested in the potential dispute, as it may not like the result. Chance of dispute initiated by the counterparty is small, since the money is kept on a smart contract and the party has no control over it.

The party creates a deal at jury.online, with money for the work deposited to the deal balance. When creating the deal, the party specifies that in case of a dispute, the counterparty covers 80% of litigation expenses, making a payment in advance. This ensures that the party will bear no losses if the counterparty does not do the job. The party itself pays 20%, being a guarantee for the counterparty that the party will not dispute the deal regardless of its result. This ratio (80% to 20%) is not mandatory and may vary.

Moreover, the counterparty can make an additional deposit as a guarantee of immediate high-quality result. In this case, the party may pay for the proceedings.

- Counterparties are residents of two faraway countries representing big companies and willing to execute a deal, e.g. goods delivery. However, they understand that if something goes wrong, fees for litigation in other country will be significant. In this case, the deal with classic dispute resolution is too risky, and the game is not worth the candle.

- Payment prolongation and warranty cases. Imagine you want to buy a TV, you find a seller, buy the TV and bring it home. It's working fine, but in a week it fails to show anything, and the seller is already gone or directs you to the repair shop. Use of Jury.online platform would force the seller to be interested in resolution of such a case.

Money can be transferred after the product has been delivered and used for some time, or any other work can be paid for after proper testing and examination. The payment can be divided into parts with the next part coming only after the previous obligation is fulfilled.

- Jobs for experts. There are many highly-qualified diverse specialists all around the world who have skills, experience and personal point of view concerning field-specific questions which are out of the competence of regular jurors. Thousands of these experts are currently unemployed and have no chance to take part in dispute resolution and get money for their job though they are knowledgeable enough in the topics considered in courts. Jury.online helps people earn money with their knowledge, competence, skills, experience and independence of mind.

The list of applications may be continued with million of other cases.

3 Jury.online protocol

The protocol is a description of a smart contract operation, its specification for deal execution and resolution. The protocol defines interaction of counterparties, judges and pools of judges, as well as requirements for information encryption and side channel communication.

The protocol is open to the public which can adjust and develop it, search for possible vulnerabilities and make suggestions.

Described below are general ideas and requirements, while full description is available in the technical whitepaper.

Clear understanding of the following subsections requires familiarity with cryptographic primitives, such as public-key cryptography, cryptographic hash functions, and pseudorandom number generators. Explanation of these

topics goes beyond the purpose of this document and Wikipedia articles provide enough insight for further reading [5, 3, 4].

3.1 Requirements for participants

All participants — counterparties, judges, pool operators — must have a pair of keys used in asymmetric cryptosystem for their identification and to sign their actions. Such a key pair is given to every owner of an “account” of a typical blockchain.

3.2 Attachements

Counterparties of the deal need a secure way to share files and documents, and these attachments later must be exposed to the judges. Moreover, the jurors need complete information about all actions, and they also need to be sure that the files presented were really sent by a certain counterparty. Fortunately, modern cryptography successfully solves this problem via good old asymmetric cryptosystems. During a dispute resolution, the counterparties decide which documents are vital for the correct outcome and disclose them to the jurors.

3.3 Smart contract of a deal

Described below are requirements for a smart contract, information it stores, functions to be called and participants to call them when the deal becomes active.

Smart contract stores the following information:

1. Counterparty identifiers
2. Subject of the deal, links to related documents and attachments.
3. Starting time of the deal, time for execution, time for acceptance, the moment of dispute fee payment.
4. Counterparties’ deposits and collateral for dispute resolution.

5. Type of dispute resolution, e.g. identifier of the pool of judges for random judges.
6. Identifiers of other smart contracts used in the protocol:
 - (a) rating smart contract (Rater)
 - (b) chooser responsible for choosing a judge, based on a random number generator (RNG)

This data is vital for smart contract operation, but typically it would hold more information, e.g. information about public visibility of the deal at the website or number of possible appeals.

3.4 Multiparty deals

In fact a deal is just an obligation statement agreed with all involved parties. Generalization of the case with two parties to the greater number of participating sides encounters no new fundamental problems. However, on the contrary to the case with only two parties, multilateral deals must prescribe more detailed behaviour in possible outcomes, because determining the “wrong” in general would not result in automatical determination of the “right”.

For instance imagine a customer who needs a website. He finds a designer, backend developer and frontend developer, and all of them agree to work together. Customer makes a deposit for complete website partitioned for all workers. In case one of the developers disappears and the rest workers fulfill their obligations, it’s not clear how to handle the deposit.

Nevertheless, with proper description of the outcomes, multiparty deal can be treated in the same way as a two-party deal. So if rules for all the outcomes are set beforehand, like “in case of one of the worker leaves, or doesn’t finish work on time, then the rest receive 80% of their payments”.

If the parties don’t form interconnected obligations, then relations between parties should be pairwise with a separate deal for each pair.

Summing up, jury.online protocol allows creation of multilateral deals, but its use is more complicated and we hardly see it as a main purpose of the system.

3.5 Requirements for pools

Pools should maintain up-to-date lists of active judges who are online and ready to consider disputes. In order for a smart contract to know them, part or all of the information about the list should be kept in the blockchain.

Depending on the price of transactions in the blockchain, there are at least two mechanisms of storing up-to-date information:

- Storing identifiers of all judges directly in the blockchain. In this case, however, keeping the list updated might be expensive as it requires sending transactions to the blockchain.
- Publishing cryptographic hash of the list in the blockchain. While the list is provided by the pool on their website, Jury.online application or a user themselves can verify that the provided list corresponds to the published hash.

3.6 Selection of judges

Basic services include random selection of judges for dispute resolution. Pools provide up-to-date lists of active judges. In case of a dispute, a pseudorandom number generator selects the required number k of specific judges from this list who receive information about the deal. Random number generator operates via smart contract so that it is not controlled by any party. However, for operation it needs some initial state that is defined by a numeric parameter called seed. Since all information in the blockchain is open and accessible to any user, a pool operator or a party that knows the seed can adjust the judges' order so that a certain deal is considered by certain judges who may be in collusion with a party. Therefore, seed cannot be calculated on the basis of any public information but should use parameters provided by the counterparties. Since counterparties to a dispute pursue opposite goals, they are interested in safe and high-quality seed that would lead to an unpredictable judge choice.

3.7 Summary of the working scheme

1. Counterparties generate random integer numbers a, b in the range of $0..2^{256} - 1$.
2. Counterparties calculate the cryptographic hash of these numbers:

$$A = \text{hash}(a)$$

$$B = \text{hash}(b)$$

3. Counterparties send A, B to the smart contract of the random number generator.
4. Counterparties send a, b to the smart contract of the random number generator, and it checks that previously sent hashes are indeed of these numbers:

$$A = \text{hash}(a)$$

$$B = \text{hash}(b)$$

If one of the equalities is false, it means that a counterparty is trying to deceive the system and choose non-random judges. In this case, the counterparty becomes a losing party, and the dispute is resolved in favor of the other party.

5. Smart contract calculates seed using both numbers a, b , for instance:

$$\text{seed} = \text{hash}(a\|b),$$

where $\|$ denotes concatenation.

6. Based on the calculated seed, the generator produces the required random numbers i_1, i_2, \dots, i_k identifying judges from the pool.

$$[i_1, i_2, \dots, i_k] = \text{prng}(\text{seed}, k)$$

7. After calculating identifiers of random judges, smart contract of the random number generator sends them to the smart contract of the deal.

What is ensured this way? As order of sending numbers a , b cannot be regulated, the counterparty that is second to send them can adjust its numbers so that the seed has a certain special form resulting in generation of identifiers of the judges affiliated with it. Thus, hash sending guarantees that after the numbers are selected they cannot be changed neither by the deal party nor by the pool operator.

3.8 Judges' verdicts

Economic and rating motivation forces judges to investigate and resolve disputes fairly and correctly, rather than to randomly pass their verdicts. Judges should not know verdicts of other judges to prevent them from taking the decision voted for by a majority. Therefore, a mechanism for hiding the verdicts must be used, and verdicts cannot be stored in the blockchain as the number of for/against votes.

Jury.online uses probabilistic encryption This method has one important feature: cipher text doesn't

In short

The algorithm used her Verdict is encrypted with some additional randomly generated data — “salt”. This data is generated by the parties of the deal. Parties to encrypt the verdict are chosen in rotation.

Party uses symmetric-key algorithm to encrypt the salt and to store it in the smart contract of the deal. Later the party will disclose the encryption key and reveal the verdict. Refusal to disclose the key would mean that this party lost the dispute.

Then a party encrypts the salt using judge's public key and sends it to the judge via side channel, so it's not published in the blockchain. Judge can reveal the salt and make their verdict open, however it can be done only by publishing their private key, so the judge will lose control of their account and all funds at its balance.

Another approach is to use probabilistic encryption, though it's rather complicated and is therefore described in the technical whitepaper and protocol specification there. A significant advantage of this method is that there is no need in side channel communication.

3.9 Ratings

Rating system is vital for correct operation, because dispute resolution price is based on the judges' competence. Estimation of someone's competence is a very nontrivial task, and it's evaluated by a number of statistical methods that provide resulting numerical parameter — rating.

As we want rating to be fair and uncontrollable by anyone, it's implemented via smart contracts, so it's automatically recalculated after any of the parameter has changed. Along with a rating system, there are some open metrics which can be used for judge assessment and choice. E. g. a party wants a potential dispute to be settled by a group of jurors who have average response time less than 2 hours and total money earned more than equivalent of \$10 000.

List of these metrics is given below. Counterparty participant:

- Number of deals they participated in.
- Number of deals resulting in a dispute.
- Number (ratio) of disputes won.
- Money spent on deals/disputes.
- Frequency of deal creation

Judge participant:

1. Number of disputes they participated in.
2. Number (ratio) of disputes won, i.e. number of disputes where they took a decision that became final.
3. Amount of money earned through the system.
4. Average (median, modal) time of decision making.
5. Average (median, modal) availability, i.e. how often they are online and ready for dispute resolution.
6. Pairwise judge-counterparty metrics, i.e. how many times this judge participated in disputes of a certain counterparty.
7. Number of appeals won or lost.

Both counterparties and judges rate each other, but these metrics are not used to evaluate anyone's competence and are shown just as additional parameter.

4 Jury.online platform

Jury.online implements the above-mentioned protocol on the basis of Ethereum blockchain connecting counterparties and judges.

4.1 Operation

Unfortunately, working with blockchain is still challenging for people unaware of technical details. For normal operation, one needs to have the entire Ethereum blockchain which currently occupies 290 GB of memory[1]. Of course, it is too much for an average user, not to mention mobile devices. Therefore, jury.online operates as an intermediary enabling users to send transactions to the blockchain. Transactions cannot be changed by jury.online due to the absence of users' private keys.

Jury.online keeps its own nodes and servers for flawless service operation, and the user doesn't have to manually call contracts functions through parity or mist. The user visits the website or mobile application, performs an action which is translated into blockchain transaction and signs it by their private key stored on their side.

4.2 Connection of pools

Jury.online provides various organizations, companies and groups of specialists with the opportunity to offer their dispute resolution services. After verification and audit, jury.online "issues a license" to the pool and includes this pool into the list of those publicly available when a deal is created. Jury.online publishes statistics and average user ratings when using this pool. In case of unsatisfactory operation, the license is revoked. Also note that pool of judges is selected by counterparties and not imposed by jury.online.

4.3 Economy

Cryptocurrencies transfer arises in the workflow in following forms:

1. Transaction fee of the blockchain¹.

This part is paid by the initiator of the deal. By agreement with the other counterparty this fee can count as a part of the deal sum.

2. Deal amount.

Both counterparties may deposit funds to the smart contract of the deal. Hence, counterparty that is meant to receive the deal amount may provide a pledge to show their serious altitude to the deal.

3. Dispute resolution payment

This part must be paid in order to start the dispute. As in dispute there is at least one dissatisfied party, we expect exactly this party to provide this payment.

The first two items are nominated in the internal blockchain cryptocurrency. Jury.online has no control on these amounts and takes no commission from these parts.

Jury online takes commission only from dispute resolution payment, the third item from the list. Dispute resolution fee is paid in Jury.online Tokens (JOT) which are issued at the ICO. Fee is only charged in case of resolution, so a deal without a dispute takes no other fee than that for blockchain transaction.

So jury.online receives the same fee both for the \$10 000 deal and \$100 deal. However, we expect that \$10 000 deal requires more qualified jurors for dispute resolution, hence it will have larger dispute resolution payment.

Moment of fee payment is specified beforehand, so a deal can be created with tokens deposited for a potential dispute, or tokens can be purchased when the dispute is started. If the deal is successfully executed without dispute, tokens are returned back to the party that provided them.

¹If there is any fee for transaction in the underlying blockchain

4.4 Jury.online commission

This commission is used for platform maintenance and further development. Maximum commission is 20%, while minimum is 0%.

Rules are as follows:

- First 1000 resolutions have 0% commission, with all the tokens deposited going to the judges
- Next 9000 resolutions require 10% commission
- Subsequent resolutions require 20% commission, though this value may be decreased depending on the circumstances (e.g. discount, sale, etc.).

JOT is also used to pay for pool audit and verification, as well as for the issue of a “pool license”.

JOT can be bought at cryptocurrency exchanges or directly from the Jury.online (if it has any JOT supply).

4.5 Appeals

Anything in our world can be thought from a different point of view, no judge can satisfy everyone’s expectation and fit everyone’s concept of justice. Judges’ work is to provide unbiased and just verdict, but the judge is not a superhuman, may make mistakes as any other person. However, review of a verdict by “more qualified” juror and repeating this process of reviewing judge’s verdict by a superordinate judge makes the probability of error sufficiently small.

Counterparties of the deal may agree on the potential appeals for the deal. Appeal is in essence just a dispute about the verdicts of the initial dispute. Every judge providing his verdict supplies it with his arguments and comments, why and how he came up with his decision. Later, a judge of a higher rank involved in appeal reviews these comments and arguments and makes his own decision.

If a judge’s verdict is found to be wrong by supreme instance, judge loses his payment and rating. Such a loss is more severe than that of just being wrong.

4.6 Protocol development, research

Presented protocol is not final, it will be improved. Current version is blockchain-agnostic, and our implementation uses Ethereum, as it's the most convenient blockchain with Turing-complete smart-contracts today. While the blockchain technology is widely spreading today, we may use some other blockchain if its properties fit the protocol needs better than Ethereum.

5 Features

5.1 Escrow

Escrow is the most important feature. Money is not transferred immediately but stored by a third party, in this case, on a smart contract in the blockchain that is completely independent and operates based exclusively on the code of that contract.

5.2 Jury market

We turn court judgements into a market. You can always figure out what is more expensive: to start litigation or not to start. Jurors provide price for which they are ready to work, so the counterparties know in advance how much a potential dispute would cost and may accurately estimate their risks.

5.3 Jury pools

Use of the platform and protocol is impossible without judges, so we give third-party companies the opportunity to provide judges for dispute resolution (even quite specific ones).

5.4 Customization of dispute resolution

As it was stated in the problems list, modern disputes are hardly connected with jurisdictions, and people have no choice in how their dispute should be resolved. jury.online offers a range of opportunities:

1. Judges from a general-purpose pool working on disputes that require no particular skills or specific knowledge. These judges remain anonymous to prevent colluding.
2. Judges who are specialists in a certain industry. Of course, their services would cost more compared to those of non-experts.
3. A person or a group of people known to be impartial professionals in a certain sphere credible in opinion of all the counterparties — these judges are open and their names are not kept in secret.
4. Each counterparty may have their own judges, more or less affiliated with them. However, the other party is entitled to reject some of the persons on the list.

Additional features:

- Opportunity to reject a number of judges proposed, if the counterparty considers they are not fair. The greater the number of judges rejected, the higher the cost.
- Before the deal is started, counterparties may provide their set of laws, i.e. set of characteristics that should be used to estimate the deal execution.
- Pairwise judge-counterparty statistics to show that a certain judge is not affiliated with a certain counterparty.

5.5 Integration

There are plenty of companies that need dispute resolution services: online stores, freelance platforms, marketplaces. For instance, instead of having their own dispute resolution department Amazon or Upwork could outsource this service to jury.online platform.

Any party with such a need can assure their customers that the service provided is fair, and should any dispute arise, it would be considered by unprejudiced jurors.

Set or rules for connecting the service to jury.online system is being developed now and will later be published at jury.online website.

After the integration with jury.online third parties may list dispute statistics information of a certain user in order to have additional metrics for reputation systems and proficiency evaluation.

5.6 Security

The system operates based on smart-contract code, not human action which can be easily affected. It is known to any party and cannot be changed. This also applies to money transfer: money is held on the smart-contract and cannot be withdrawn in any way except after successful deal execution or dispute resolution by jurors from a pool agreed beforehand.

Every human action involves use of cryptographic keys of a participant that unambiguously identify the user. All actions are stored in blockchain transactions, and blockchain network has already proven its unwavering reliability when used for any purposes.

5.7 Paranoid mode

Paranoid mode is for the users that don't want to entrust our service with anything. For example, they may be afraid that we could censor their transaction and their action would not be broadcasted into blockchain on time, which is the only possible way to interrupt the contract operation, as jury.online cannot fake a blockchain transaction and corrupt the user's intent.

Paranoid mode involves a toolkit with open source code along with a set of instructions on how to use the platform without any third party. However, this way requires user to have a blockchain node and to call all the smart contract functions by themselves, which is rather nontrivial for an inexperienced user.

5.8 Statistics

Jury.online platform operation involves a statistics contract which counts the following data about overall platform operation:

- Number of deals created
- Number of disputes opened
- Total sum of collaterals transferred
- Total sum of tokens used for dispute resolution (total sum of JOTs earned by jurors).

5.9 Audit

We provide selective audit of deals, judges and disputes by administration of jury.online. We would consider random deals and disputes and rate their resolutions by ourselves. It would not change ratings, as rating system is based on decentralized smart-contracts, but any users at the website or application would see additional verification mark of our own assessment at a person's profile.

6 Initial coin offering

ICO will have the following stages:

1. Presale. Up to the 20% of all tokens available to public will be allocated with a 30% discount during an 11-day presale.

Presale limit: 20% of all tokens for sale = 4 200 000 JOT (up to 14 000 ETH)

Price: 1 ETH = 300 JOT (1 JOT \approx 0.0033 ETH).

Minimal amount of tokens to be bought: 500 JOT (\approx 1.67 ETH).

Dates: 23 October 14:00 UTC - 03 November 2017 14:00 UTC.

2. Sale Price: $1 \text{ ETH} = 210 \text{ JOT}$ ($1 \text{ JOT} \approx 0.0048 \text{ ETH}$).

Minimal contribution: 5 JOT.

Time bonuses for early contributors will start from 20% discount on the first day with linear daily decrease by $\frac{2}{3}\%$ (2 percent for 3 days).

Dates: 13 November 14:00 UTC - 13 December 14:00 UTC.

Total maximum supply of JOT: 30 000 000.

For every 7 JOTs sold through ICO jury.online issues 3 JOTs for itself.

Thus, up to 21 000 000 JOT will be available for public and up to 9 000 000 JOT will be reserved by jury.online.

21 000 000 JOT available to public is divided into:

1. Presale supply: 4 200 000
2. Sale supply: 16 800 000

ICO minimum cap is set for overall crowdsale, sum of sale and presale stages.

ICO success: 3 000 000 JOT

Which is equal to $10\,000 \text{ ETH} \approx \3 mln during presale, $14\,285 \text{ ETH} \approx \4.29 mln during sale; with $1 \text{ ETH} \approx \$300$.

Tokens can be bought for ETH and BTC, as well as for fiat money.

Token transfer would be available only after the end of ICO.

The start and the end of each stage will be linked to specific Ethereum block numbers and will later be published at the website.

Tokens reserved by jury.online will be distributed as follows:

- 20% go to the jury.online team and will be blocked for a period of 6 months. After that period, 10% of the total amount blocked will be unblocked every month, with the whole sum therefore unblocked in 16 months after the ICO end.
- 7% go to advisers and for bounty programmes.
- 3% remain as a stock of liquidity to ensure flawless and independent operation of jury.online before token enters cryptocurrency exchanges

and the market stabilizes, as well as for compensations in exceptional cases.

7 Roadmap and milestones

- Autumn 2017: ICO
Development organization
- Spring 2018: Web version alpha release
Basic features (deals with random judges, one pool) released.
Testing, start of operation, creation of “general-purpose” pool.
- Summer 2018: Mobile applications release.
- Summer 2018: Implementing the full set of features (various resolution types, paranoid mode).
- Summer-Autumn 2018: Third-party pools opening.
- Autumn 2018: Development of third-party services integration infrastructure.
- Winter 2018-2019: Start of integration with third-party services (e.g. Upwork, Amazon).

8 Epilogue

Smart contracts are digital contracts, written in code with clauses enforced automatically. World just starts to explore how to apply this technology. Yet, smart contracts have a lurking problem: transforming human intention into a smart contract code is a great challenge. And as our world is getting more complicated so do our desires, such a complication would require more refined and powerful techniques.

Luckily, when properly motivated, humans can be intelligent, flexible, fair, and reasonable: exactly the qualities that bad code lacks. This suggests

that until we know how to express our desires in a not human-oriented way, we have to create systems which benefit from both human and machine expertises to maximize the result.

So Jury.online is neither a new blockchain nor an old service which attempts to integrate blockchain. Jury.online is a project which aims to use the full power of contemporary technologies to solve problems that were considered unsolvable for decades.

References

- [1] Etherscan. The Ethereum Block Explorer.
- [2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system,” <http://bitcoin.org/bitcoin.pdf>.
- [3] Wikipedia. Cryptographic hash function — wikipedia, the free encyclopedia, 2017.
- [4] Wikipedia. Pseudorandom number generator — wikipedia, the free encyclopedia, 2017.
- [5] Wikipedia. Public-key cryptography — wikipedia, the free encyclopedia, 2017.