



JURY.ONLINE

Jury.online

Alexander Shevtsov

Contents

1	Introduction	2
1.1	History	2
1.2	Problems	3
1.3	Objectives	3
1.4	Blockchain	4
2	Description	5
2.1	Overview	5
2.2	Operation	5
2.3	Use cases	6
3	The Jury.online Protocol	8
3.1	Requirements for Participants	8
3.2	Attachements	9
3.3	The Smart Contract of a Deal	9
3.4	Multiparty Deals	10
3.5	Requirements for Pools	11
3.6	Judge Selection	11
3.7	Operation Summary	12
3.8	Judges' Verdicts	13
3.9	Ratings	14
4	The Jury.online Platform	15
4.1	Operation	15
4.2	Adding Pools	15
4.3	Economy	16
4.4	Jury.online Commission	17
4.5	Appeals	17
4.6	Protocol Development and Research	18
5	Features	18
5.1	Escrow	18
5.2	Jury Market	18
5.3	Jury Pools	19
5.4	Customization of Dispute Resolution	19
5.5	Integration	20

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	24

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, as has been the case since commodity trading markets evolved millennia ago in Mesopotamia, trust still remains paramount in business relationships and global trade today.

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 do not yet correspond to the realities of the modern world and existing legal cases have clogged the already overburdened judicial system, which has coincided with a steep rise in the cost of legal services and litigation.

Let's take a look at the contemporary problems in 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Modern litigation or other kinds of dispute resolution are completely outdated and have a number of fundamental disadvantages: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 lawyer's fees for civil lawsuits can run up to thousands of dollars.
- Duration of proceedings. As a rule, it takes several court sessions at intervals of 1-2 months to solve a case. That, of course, is too long for most disputes.
- Judgement execution. 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 avoid fulfilling its obligations.
- High entry requirements. Most often, only big cases are heard in courts, and few people are ready to start serious litigation for disputes over everyday matters like a poor-quality product or service. The cost and complexity of proceedings do not depend too much on the subject of the deal.
- Jurisdictions. Public courts administer justice under the laws of a certain state, which vary significantly between countries.
- Political engagement and bias. Courts are not always independent — they are often influenced by other institutions and people.
- Complexity. Few people can protect their own interests; for the rest, trials are very complicated.
- Lack of choice. There is no way to choose the 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 the current execution and regulation of deals to be completely outdated and want to change this by creating a protocol for interaction between judges and the

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 started to spread in 2008[2]. A blockchain is a ledger of information blocks with built-in fault tolerance and the absence of centralized control. It can be thought of as a decentralized database with distinct update rules. Today, blockchain is the best tool for solving trust and security problems.

The information stored in a blockchain network is open, since the common database simultaneously exists on all computers that are part of the network. All changes to the blockchain are carried out on a stage-by-stage basis by means of transactions, each of them open to everybody. The blockchain cannot be corrupted, since all changes made should satisfy the rules that are predefined by the protocol specification developed by the 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 the 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 is 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 that, if any party is dissatisfied, are reviewed by a panel of jurors that deliver a judgement in favour of one of the parties. Jury.online also gives any person with expertise in a certain field the 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-made templates, specifying all the 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 smart contracts. In addition, the deal is assigned a link that leads to a webpage displaying information about it. 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, if a deal is intended for product or service delivery, but the initiator does not yet 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 receive, 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 or not and whether the parties were content with its execution or need to start legal proceedings. Part of the balance is allocated to resolving possible disputes, i.e. paying court fees (this is 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 necessary information, the deal is considered to be concluded.

After that, the parties have a certain period of time to fulfil their obligations. In the event that each party is satisfied with the result, the money from the 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 that one of the parties is not satisfied with the execution of the deal and believes that the counterparty has not fulfilled its obligations, the deal is sent to the judges for examination. Any party may initiate a dispute and send the deal to the judges, but as a rule it is the party that deposited money.

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

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

Judges are provided from a source called a judge pool: most simply, this is done by jury.online, but third parties specializing in a certain field may also offer dispute resolution services. The identity of judges is not known to the parties, but their competence is. Judges have a fixed period of time to make a decision. Information about the decision of a particular judge is encrypted and unavailable to other judges. Other forms of judging are accessible: instead of several random, unknown judges, the parties may agree on a specific judge they consider fair and impartial. Most deals imply the performance of contractual obligations for a payment. In this case, one party has automatically fulfilled its obligations, as it has transferred the payment to a smart contract, so it would be the only party interested in a 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 is to pay for possible litigation and when.

2.3 Use cases

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

- One party is a company that needs to design a logo or write a text

according to certain terms of reference. The company is quite well known and pays well, thus expects the works to be performed to the required quality. The counterparty is an artist without any outstanding works who has not used the 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 first party is the one interested in a potential dispute, as it may not like the result. The chance of a 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 on 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 payment in advance. This ensures that the first party will bear no losses if the counterparty does not do the job. The party itself pays 20%, guaranteeing to 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 an immediate guarantee of a high-quality result. In this case, the party may pay for dispute proceedings.

- The counterparties are residents of two distant countries representing large companies who wish to execute a deal, e.g. goods delivery. However, they understand that if something goes wrong, fees for litigation in the other country will be significant. In this case, a deal with classic dispute resolution is not worth the risk.
- Payment prolongation and warranty cases. Imagine that you want to buy a TV: you find a seller, buy the TV and bring it home. Everything seems fine, but it stops working a week later and the seller has already disappeared or directs you to a repair shop. Use of the jury.online platform would force the seller to be interested in resolving 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 has been fulfilled.

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

This list of applications may be complemented with millions of other usage cases.

3 The Jury.online Protocol

The protocol is a description of a smart contract operation and its specification for deal execution and resolution. The protocol defines the interactions between counterparties, judges and pools of judges, as well as the 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 the general ideas and requirements, while a full description is available in the Technical Whitepaper.

A 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 and pool operators — must have a pair of keys used in an asymmetric cryptosystem for their identification and

to sign their actions. Such a key pair is given to every owner of an “account” in a typical blockchain.

3.2 Attachements

Counterparties of the deal need a secure way to share files and documents, and these attachments must later be revealed to the judges. Moreover, the jurors need complete information about all actions, and they 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 dispute resolution, the counterparties decide which documents are vital for the correct outcome and disclose them to the jurors.

3.3 The Smart Contract of a Deal

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

A smart contract stores the following information:

1. Counterparty identifiers.
2. The subject of the deal, as well as links to related documents and attachments.
3. Starting time of the deal, the time for execution, time for acceptance and 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) selector responsible for choosing a judge, based on a random number generator (RNG)

This data is essential, but a smart contract would typically hold more information, e.g. on the public visibility of the deal on the website or the number of possible appeals.

3.4 Multiparty Deals

In fact, a deal is just a statement of obligations agreed between all involved parties. No fundamental problems are encountered when extending a case with two parties to a greater number of participants. However, unlike a case with only two parties, multilateral deals must prescribe more detailed behaviour in each of the possible outcomes, because in general determining who is “wrong” does not automatically determine who is “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. The customer makes a deposit for a complete website partitioned between all the workers. If one of the developers disappears and the other workers fulfil their obligations, it is not clear how to handle the deposit.

Nevertheless, with proper description of the outcomes, a multiparty deal can be treated in the same way as a two-party deal — if rules for all the outcomes are set beforehand, e.g. “in case one of the workers leaves or does not finish their work on time, the rest receive 80% of their payments”.

If the parties do not have interconnected obligations, relations between parties should be organised in a pairwise manner, with a separate deal for each pair.

To sum up, the jury.online protocol allows for creation of multilateral deals, but this 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 review disputes. In order for a smart contract to know this, 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 may be expensive, as it requires sending transactions to the blockchain.
- Publishing a cryptographic hash of the list in the blockchain. The list is provided by the pool on their website and the Jury.online application or a user can independently verify that the list corresponds to the published hash.

3.6 Judge Selection

Basic services include the 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 to receive information about the deal. The random number generator operates via smart contract so that it is not controlled by any party. However, it requires an initial state that is defined by a numeric parameter called a “seed”. Since all information in the blockchain is open and accessible to any user, a pool operator or party that knows the seed can adjust the order of judges so that a certain deal is examined by certain judges who may be in collusion with a party. Therefore, the seed cannot be calculated on the basis of any public information — it should use parameters provided by the counterparties. Since the counterparties to a dispute pursue contrasting goals, they are interested in having a safe, high-quality seed that ensures an unpredictable choice of judges.

3.7 Operation Summary

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

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

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

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

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

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

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

5. The smart contract calculates a 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 that identify judges from the pool.

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

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

What does this approach ensure? As the order in which numbers a and b are sent cannot be regulated, the counterparty that is second to send them could adjust its numbers to make the seed have a certain form that would generate the identifiers of judges affiliated with it. Therefore, sending the hashes guarantees that the numbers cannot be changed by either a party to the deal or the pool operator after they have been selected.

3.8 Judges' Verdicts

Economic motivation and ratings force judges to investigate and resolve disputes fairly and correctly, rather than randomly returning their verdicts. Judges should not know the verdicts of other judges — this prevents them from simply agreeing with the decision voted for by the majority. Therefore, a mechanism for hiding the verdicts must be applied and verdicts cannot be stored in the blockchain as a number of votes for/against.

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

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

As we want the rating to be fair and uncontrollable by anyone, it is implemented via smart contracts, so that it is automatically recalculated after any of the parameters is changed. Alongside the rating system, other open metrics can be used for judge assessment and selection. For example, a party wants a potential dispute to be settled by a group of arbiters who have an average response time of less than 2 hours and total money earned equivalent to more than \$10 000.

A list of these metrics is given below. Counterparty participant:

- Number of deals 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 participated in.
2. Number (ratio) of disputes won, i.e. number of disputes where their verdict corresponded to the final decision.
3. Amount of money earned through the system.
4. Average (median, modal) time for decision-making.
5. Average (median, modal) availability, i.e. how often they are online and ready to resolve disputes.
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 just shown as an additional parameter.

4 The Jury.online Platform

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

4.1 Operation

Unfortunately, working with blockchain is still challenging for people unaware of the technical details. For normal operation, one needs to store the entire Ethereum blockchain which currently occupies 290 GB of memory[1]. Of course, this 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 maintains its own nodes and servers for flawless operation of the service, while the user does not have to manually call contract functions using Ethereum clients. The user visits the website or mobile application, performs an action that is translated into a blockchain transaction and signs it with their locally stored private key.

4.2 Adding Pools

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

4.3 Economy

Cryptocurrency 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 party, this fee can be counted as a part of the deal amount.

2. Deal amount.

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

3. Dispute resolution payment

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

The first two items are denominated in the internal blockchain cryptocurrency. Jury.online has no control over these amounts and takes no commission from them.

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

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

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

¹If there is any transaction fee in the underlying blockchain

4.4 Jury.online Commission

This commission is used for platform maintenance and its further development. The maximum commission is 20%, while the minimum is 0%.

The rules are as follows:

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

Half of commission received “is burned” in sen

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

JOT can be bought on cryptocurrency exchanges or directly from Jury.online (if it has any JOT available).

4.5 Appeals

Anything in our world can be thought of from a different point of view — no judge can satisfy everyone’s expectations and fit everyone’s concept of justice. The judges’ job is to provide an unbiased and just verdict, but a judge is not superhuman and may make mistakes, just like any other person. However, the review of a verdict by a “more qualified” arbiter and repetition of this process by higher ranked judge makes the probability of error sufficiently small.

Counterparties to a deal may agree on potential appeals for the deal. An appeal is in essence just a dispute about the verdicts of an initial dispute. Every judge providing a verdict supplements it with their arguments and comments on why and how they came to their decision. Later, a judge of a higher rank involved in appeal reviews these comments and arguments to make their own decision.

If a judge’s verdict is found to be wrong by a supreme instance, the judge loses their payment and rating. Such a loss is much more severe than that of simply being “wrong”.

4.6 Protocol Development and Research

The presented protocol is not final and will be improved. The current version is blockchain-agnostic and our implementation uses Ethereum, as it is currently the most convenient blockchain with Turing-complete smart-contracts today. As the blockchain technology is widely spreading today, we may use another blockchain if its properties fit the protocol’s 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, 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. It is always possible to figure out what will be more expensive: to start litigation or not. Jurors provide the price for which they are willing 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 was stated in the list of problems, modern disputes are rigidly connected to jurisdictions, and people have no choice in how their dispute is 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 collusion.
2. Judges who are specialists in a certain industry. Of course, their services would cost more than those of non-experts.
3. A person or group of people known to be impartial professionals in a certain field and who are credible in the opinion of all counterparties — information on these judges is open and their names are not kept 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:

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

5.5 Integration

Many companies need dispute resolution services: online stores, freelance platforms, marketplaces and so on. For instance, instead of having their own dispute resolution department, Amazon or Upwork could outsource this service to the 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 will be examined by unprejudiced jurors.

A set of rules for connecting the service to jury.online system is currently being developed and will later be published on the <http://jury.online> website.

After integration with jury.online third parties may list information on the dispute statistics 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 influenced. The code is known to all parties and cannot be changed. This also applies to money transfers: the money is held on the smart-contract and cannot be withdrawn in any way, except after the successful execution of the deal or dispute resolution by jurors from a pool agreed on in advance.

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

5.7 Paranoid Mode

Paranoid mode is for users that do not want to entrust our service with anything. For example, they may be afraid that we could censor their transaction and their action will not be broadcasted into the blockchain on time, which is

the only possible way to interrupt a contract operation, as jury.online cannot fake a blockchain transaction and distort the user's intentions.

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

5.8 Statistics

The jury.online platform includes a statistics contract that records the following data on overall platform operation:

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

5.9 Audit

The administration of jury.online selectively audits deals, judges and disputes. We will consider random deals and disputes, and rate their resolutions by ourselves. This will not change the ratings, as the rating system is based on decentralized smart contracts, but any users at the website or application will see an additional verification mark on a person's profile from our own assessments.

6 Initial Coin Offering

The ICO will have the following stages:

1. **Presale.**

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

Presale limit: 30% of all tokens for sale = 2 100 000 JOT (up to 7 000 ETH)

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

Dates: 23 October, 14:00 UTC — 03 November 2017, 14:00 UTC.

2. **Sale.**

Price: 1 ETH = 210 JOT (1 JOT \approx 0.0048 ETH).

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

Dates: 12 February, 14:00 UTC — 14 March, 14:00 UTC.

Total maximum supply of JOT: 10 000 000.

For every 7 JOT sold through the ICO jury.online will issue 3 JOT for itself.

Thus, up to 7 000 000 JOT will be available for the public and up to 3 000 000 JOT will be reserved by jury.online.

The 7 000 000 JOT available to public is divided into:

1. Presale supply: 2 100 000
2. Sale supply: 4 900 000

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 ETH \approx \$3m during presale, 14 285 ETH \approx \$4.29m during sale; with 1 ETH \approx \$300.

Tokens can be bought for ETH and BTC, as well as for fiat money².

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

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

²Only during sale stage

The 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 end of the ICO.
- 7% go to advisers and for bounty programmes.
- 3% remain as a stock of liquidity to ensure the flawless and independent operation of jury.online before the 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 automatically enforced clauses. The World is just starting to explore how this technology can be applied. Yet, smart contracts have a lurking problem: transforming human intention into a smart contract code is a great challenge. As our world becomes more complicated so do our desires, this issue requires 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 the expertise of both humans and machines in order to maximize the result.

So, Jury.online is neither a new blockchain nor an old service that is attempting to integrate blockchain. Jury.online is a project that 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.