Evidence Standardization

Proposal

[See the proposal on this file](#).

Introduction

This document is made for brainstorming and then proposal of the evidence standard which should follow the [ERC792 Arbitration Standard](#).
Evidence is to be considered in a broad sense. The plain English contract between party is a specific kind of evidence.

The purpose for creating a standard for evidence in dispute resolution is to ensure that evidence can be properly verified, secured and displayed to arbitrators across use-cases and dispute types. Evidence is crucial in allowing arbitrators to make informed rulings so it is important that it is standardized such that evidence is presented as fairly and clearly as possible for all parties involved in the dispute. In addition to standardized evidence there is dispute metadata that should be standardized as well. This meta-evidence is used to give jurors additional context for the dispute and provide clarity on their task.

Evidence needs to include a reference to an event log on the blockchain that verifies the submission and the submitter of the evidence. This event log should include some verifiable URI to the evidence. This is used to verify that the evidence has not been tampered with. The evidence should include the data referenced in the event log as well as the type of the data. The type can be one of: image, text, link, or meta. The type is used to help validate the data and can also be used to display the evidence in the correct manner so the jurors can easily and accurately use it. Lastly evidence should include a title and description to explain the purpose of the evidence and how it relates to the dispute.

Meta-evidence is used to embellish the dispute with relevant descriptors so that it is clear what choices and actions a juror can take, and to provide additional context. For example meta-evidence can specify labels for the ruling options, so that a juror can clearly understand what they are voting for. In addition to ruling option titles and descriptions, meta-evidence can include the uri of the plain text contract, user friendly aliases for ethereum addresses, and descriptions for the overarching dispute that specifies the context for the dispute (e.g. what platform it came from) and specifies the question the juror is tasked in answering.

Analysis of standardization needs

What is required for your Dapp interface. We list all the elements required by dapps and try to find a common list shared by all to be standardized. If some elements are often relevant but not always, we'll need to decide if those should be included, made optional, or not be part of the standard.

Arbitrable Transaction (Kleros POC)

- A plain English contract.
- Arbitrary evidence files: URI to a resource.
- Hash of the resource file to be stored on-chain to ensure integrity
- To have a cut-off date - when no more evidence is allowed - default timeout one week after opening a dispute.

The Doge List (curated list fun experiment)

- The picture (to be determined to be a doge or not).

Origin

- Disputes will be generally between buyers and sellers in marketplace. Examples:
    - "I never received the package"
    - "Listing said it was a size Small but I received a size Large"
    - "The apartment I rented was filthy dirty when I arrived."
    - "I *did* ship the package to buyer, and I have shipping tracking documents to prove it."
- Evidence:
    - For all disputes, a *Purchase* contract containing (at least) financial details of transaction. (Example .sol of an eBay/craigslist style purchase contract.)
    - The *Purchase* contract contains the eth address of the *Listing* contract that was purchased. (.sol of Listing contract)
    - The *Listing* contract contains a 32 byte *IPFS hash* of a data blob containing json metadata for the listing. This json is in the form of a JSON Schema and contains textual descriptions, categories, sizes, and photos. Ideally, eventually this data will be stored via FileCoin, with storage of the data paid for through the "statute of limitations" for arbitration on the listing.
        - Sample schema for "for sale" listings
        - Sample listing IPFS blob including images
        - DApp UI of same listing
    - We are using ERC725 for identity. Most buyers and sellers will have an identity contract in addition to a public ETH address.
        - Therefore, identity claims about buyer/or seller can also be evidence. For example, it might be relevant evidence to show claims of the seller having a mailing address different from what was claimed in the listing. All of these claims are stored in smart contracts that can be dereferenced from our *Purchase* contract.
    - NYI: Chat logs between buyer and seller. We are working on a prototype of this now. In general, each line of chat will be signed, including a hash of the entire conversation thus far. Thus, it can be proven that the chat is un-altered and that each actually party said what is in the log.
    - NYI: External Evidence, especially photos. E.g. in the example of a dirty apartment, the unhappy buyer could submit photographic evidence showing the condition of the apartment. This might also include photos of shipping confirmation, mail tracking, police reports, receipts, etc... Also possible this could include video or audio files. Could also be raw data files, such as computer source code, csv files, etc... Also URLs, e.g. to github repo containing a freelance contractor's code.

Ink Protocol

Listing Dispute

Possible disputes that arise when listing:

- Whether item is against the rules of the marketplace
- Whether item is legal within the jurisdiction of the marketplace
- Whether shipping price is considered “out of range” - this is important in marketplaces that only charge fees on the non-shipping portion of the price
- Whether there might be copyright infringement or other violations against intellectual property - sometimes people claim the seller is using stolen photos, or the item might infringe on someone’s copyright
- Whether the item is a counterfeit

In all these cases, we ask for evidence in the form of written statements, signed statements, copies of trademark registrations, photos, or screenshots

Purchase Dispute

Possible disputes that arise after a purchase:

- Item did not arrive
- Item arrived damaged or in bad condition (or sometimes has pet fur or smells of smoke)
- Item is not as described
- Item is fine but breaks soon after it is used
- Received empty box

Our support team typically requests the following: tracking number, other evidence of sending, such as photos or videos, shipping receipts, and finally photos of the item if needed to prove that it is broken, damaged, different than described etc.

Dether

Listing Dispute

Dether for shop:
Dether allow shop to be listed on the map.
Shop need to stake an amount of DTH (dether’s ERC20 token) to be able to do it.
They have to be inlines with their local regulation. (for example: in most country , you cant legally sell drugs)
Anyone should be able to open a dispute to verify if the shop is legal or not.

Personal app (buy and sell crypto for cash):

Our main concern is to have the possibility for both part to open a dispute, even if they don't have any ETH on their wallet. A trade will happen in different step,
0. The buyer see an ads on the map, with info about rates, volume available
1. A buyer contact a seller
2. The seller and buyer arrange for a meeting,
3. The trade physically happen, the buyer buy ETH with cash (we assume he doesn't have ETH), or the buyer buy CASH with ETH (we assume he still has ETH in his wallet), in this 2 way of trading, it's always the seller who takes the fees.
A dispute can during the step 3.
-Different scenario of dispute:
-Someone robbed me.
-The provided rates was not the one I receive.
-The transaction was mining but suddenly disappear (remplacement transaction in cash of very low fees and high network transaction)

Purchase Dispute

Recoverable Token

- Disputes can be between any two account and can be of varying natures. The nature of the Recoverable Token standard makes it hard to find an exact format for all evidence.
- Examples:
    - A friend sends tokens to another friend and before the transfer is marked as final the sender request a chargeback and the recipient disputes this request. In this case, the exact nature of the transaction will be unknown during arbitration and during the arbitration we will need to collect **testimony** from the two participants.
        - This testimony may be incomplete or partially unfactual, but the ability to collect it and decide upon its merits is needed.
        - Factors such as the credibility of a certain account holder should also be taken into account.
        - Previous transaction for each account can also be a form of evidence.
    - A friend sends tokens to another friend and before the transfer includes a hash of a document detailing the nature of the transaction. In case of a two party dispute, the document itself in addition to testimony, can be considered as evidence.

MARKET Protocol

- Disputes will be generally between traders with open positions upon expiration of a contract. Examples:
    - A contract expired based on time, but the settlement price was manipulated, was incorrect, or misreported by the oracle.

    - A contract didn't expire because an oracle callback was never received or some other bad state.
    - A Price Cap or Price Floor has been breached, but the contract was not pushed into settlement / expiration.
- Evidence for resolution
    - In the case that a contract didn't expire at the correct timestamp or contract did expire correctly based on time but the data was misreported by the oracle.
        - Market data and statistics from exchange data at expiration timestamp
    - In the case that a contract expired correctly, but the data was manipulated
        - Market data and statistics from a secondary exchange at expiration timestamp
    - In the case that a Price Cap or Floor was breached but the contract was not pushed properly into settlement / expiration
        - Market data and statistics from exchange for lifetime of contract to find time of breach

Bitnation Pangea

(Add you Dapp or dapps you think would have relevant input)

Planport Protocol

Planport is a supplychain protocol.

When a payment disputes arises within the supply chain it can to over a month to settle on top that the actual dispute the supply chain involves multiple jurisdictions and states which makes it very hard to manage disputes hence the delays. So I think with Blockchain we can reduce it very minimum while getting freelancer jurors. Supply chain consultants on demand : where we aggregate supply chain consultants on a on-demand which is a solution we have designed to tackle the big consultancy firms fees and long term contracts , so within that we see the Blockchain dispute resolution helping a lot.
So to summarise
These are our users and dispute may arise in between:
https://medium.com/planport/the-killer-application-for-the-blockchain-tech-and-planport-part-1-6515d6f6c9cc?source=linkShare-e9dc6d03286b-1531235878
-Enterprises buying side and suppliers
-Suppliers and Trade asset investors
-Enterprises and suppliers and Supply chain consultants

Problematics

Cutoff Date for evidence

How do we prevent people from submitting late evidence such that there is some information asymmetry among the arbitrators?

Possible answers

- Put a cut-off date after which the UI does not display those evidence.

Evidence Tampering

How do we prevent an evidence to be different for different arbitrators?

Possible answers

- Force the URI to contain a hash but have the interface let upload/download of the file with a user friendly name.
- Also require the evidence to contain a hash/roothash.
- Let the choice to the users to user a tamper proof naming system (like ipns) but don't force it.

Diversity of Evidence

How to deal with such diversity of evidence? How to display tailored user interface?

Possible answers

- Use json to describe the relevant data and allow UI to parse.
- Allow making read-only calls to be able to display specific values.
- Make a UI for each kind of dispute.
- Have the Arbitrator UI call the Arbitrable UI to have the same display of information.
- Allow the Arbitrator UI to make a particular rendering of evidence file it knows how to render. For the other file types, it would just allow the download of them.
- Allow javascript scripts to perform arbitrary actions (except those leading to security issues).

Meta-Evidence presentation

(plain English contract, labels, other contract informations like object bought / question of an Oracle)

- Add the function `function uriRepresentation() public view returns (string uri)` to ERC792 which would link to a URI giving the rendering of meta-evidence.

Meta-Evidence submissions

- There needs to be some restriction on who can submit meta-evidence. For example you can't have parties in the dispute or outside parties mixing up the labels on the ruling options.

If two valid parties submit meta-evidence how do you select which one to use?

- The Arbitrable contract must set up rules on how meta-evidence can be submitted to avoid this problem.

Giving proof of conversations

- Use signed messages with a public key linked to the address of the party.
- Have a specific file type containing those signed conversation that the UI would render by linking signed messages to the address/party who signed them.

Discussions

The first evidence could act as a meta-evidence, an evidence event would give the URI of the meta-evidence file (a json file whose name should be its hash). Note that the URI need not to be valid at the time this evidence is made, but should be at the time of a dispute. This is to allow better privacy for undisputed cases.
It would optionally specify:

- A short description of the dispute type (ex: "This is a escrow dispute between a buyer and a seller.", "This is a curated list dispute about whether the image represents a doge (Shiba Inu).", "This is an oracle dispute about rainfall.").
- A way to display evidence (ex: a list of files to download in the ArbitrableTransaction or a picture in the Doge List).
- The question which is asked (ex: "Who should be reimbursed?", "Is it a Doge?", "Did it rained in coordinate -0.9282393,37.0034334 the 18/04/18?").
- The title of the ruling options (ex: "The Buyer/The Seller", "Yes/No").
- A short description of the ruling options (ex: "Choose this option if there is no proof that the good was sent or if it was in bad condition. / Choose this option if the good was sent and there is no proof that the good is in bad condition.").
- A URI to the plain English contract. The file must have its name corresponding to its sha3 hash.