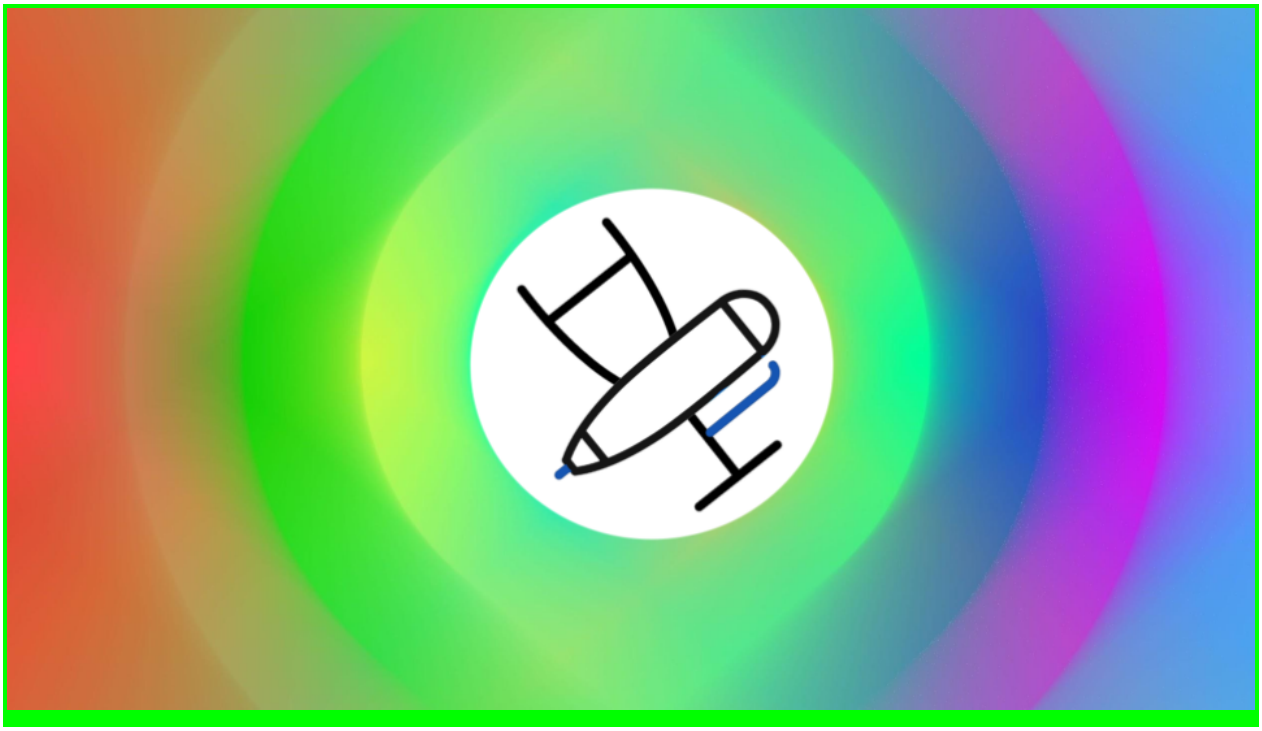


signingparty.xyz

Litepaper

27.05.2022

v0.5.11

—

hubrt.eth

Introduction

Web3 is currently mostly dealing with on-chain financial assets. But how can we process real world assets on-chain, unlocking the powers of web3 for those assets, and what kind of interactions would be necessary to accomplish that?

Connecting TradFi to the real world is mostly a legal exercise. But at web3, where code claims to be law, we run into a conundrum with interesting consequences. Blockchains learn about off-chain data via oracles. This means, you'll have to trust the integrity of the oracle service - and the source of the data the oracle is providing.

As an example: if a smart contract pays you an amount of x coins if the temperature in Berlin falls below 0° in Berlin in a specified time frame, then you'll need to trust

- the provider of the oracle to deliver clean and well documented data (is it Celsius or Fahrenheit, is it Berlin, Germany or Berlin, Ohio) ...
- the source of the data being trustworthy: is it official weather data or just a random guy pretending to read his thermometer or just a made up number?

Even wilder are the consequences with tokenized assets: we see the digital twin, but does the referenced asset even exist?

So how do we inject real world trust into the virtual but trustless blockchain world?

At its core, trust is decentralized: it's your friends and your family you're trusting, to various degrees. Locally, this works just fine. But for scale, humans need a lever. That's why we came up with brands and institutions to trust. Buying a Banksy from a random wallet address comes with some certain risks attached. Buying the same piece from Sotheby's or a well established gallery makes a difference.

Trusting brands and institutions is an age-old concept, scales really well to very high numbers, but has some shortcomings. Most importantly: those trust middlemen only scale up. They're quite well suited for the higher ends of any market. But by this, implicitly, those trust whales foster massive centralization.

We think there should be as well a decentral way to inject trust into a web3 setup, besides relying on some centralized arbiters of trustworthiness. A social approach to validate connections between the real world and web3's administrative layer.

And so we propose signingparty, a decentralized approach to trust RWA. Powered by humans, signingparty creates a Web3 of Trust, thereby enabling probabilistic proofs of existence.

On Trust

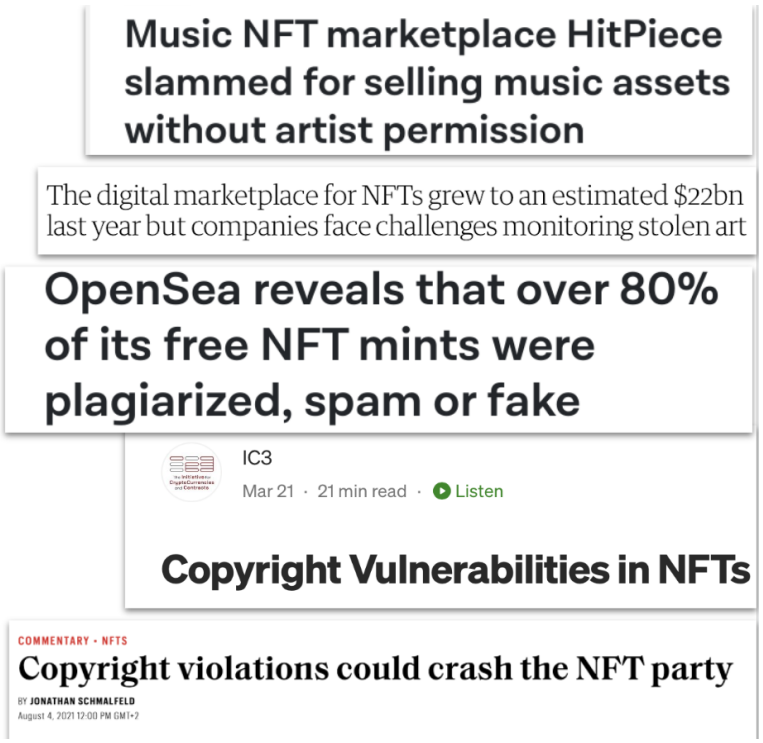
Whom to trust, what to trust.

At its core, trust is decentral: to various degrees we trust our friends and family and vice versa. Unfortunately, this graph trust doesn't scale too well. Dunbar's number says humans can relate to 150 people max. Everything else is just noise.

IRL, trust is scaled through brands and institutions. But big brands and institutions act like trust gravity wells. They suck up all fitting assets, push themselves in between asset and user and disenfranchise all creators and assets which do not fit their template of size.

For a decentralized setup, this may become critical. When dealing with RWA on chain, to trust the asset we rely solely on the issuer of the asset. This leaves us not too much middleground: either you stick to your small, but closely knitted circles - or you have to rely on the brand whales out there, vouching for the validity of the asset to be transacted.

As an example: you may be able to sell an NFT to your aunt's boyfriend. But the secondary market becomes already tricky for the buyer: is the thing I'm interested in really legit? The sheer volume of spam and fakes on the larger market places is just overwhelming.



With signingparty we're proposing a way to decentralize trust. We're scaling your networks of friends and family, augment them with a more

professional guild of signers to create graphs of dependability. Think of a web3 of trust.

Trustlessness and RWA

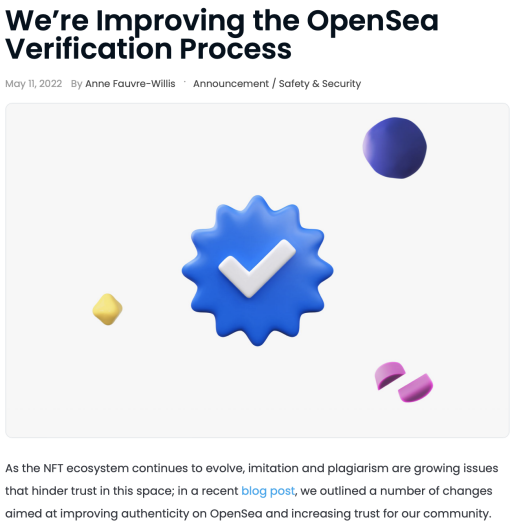
Trustless transactions, as enabled by blockchains, are a true game changer: you only have to trust the open sourced protocol and its implementation. The transaction itself will always be valid, without you having to know anything about your counterparty.

Obviously, trustlessly exchanging off-chain assets opens a whole can of worms.

- Is the minter of the asset token legitimate?
- Does the asset even exist or is it just a photoshopped scam?
- Is it just a planned rug pull around some imagery of unknown origin?

To tackle this, we need to inject some trust into the tokenization process.

Brand whales and trust hogs



Brand whales and trust hogs sit as middlemen between creators, their assets and their buyers.

An example: OpenSea, one of the leading NFT marketplaces, created a quite spam- and fake-prone environment. To tackle this, they try to entrench themselves even

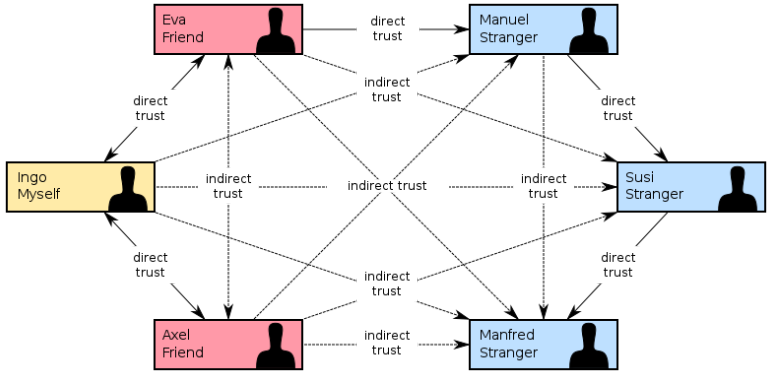
deeper into the NFT market: by becoming an institutionalized provider of authenticity.

- The protocol representing the asset itself will stay open source and standardized.
- The trust related metadata will be privately owned by OpenSea.

One more reason for a decentralized way to inject trust into web3.

People and things: a Web(3) of Trust

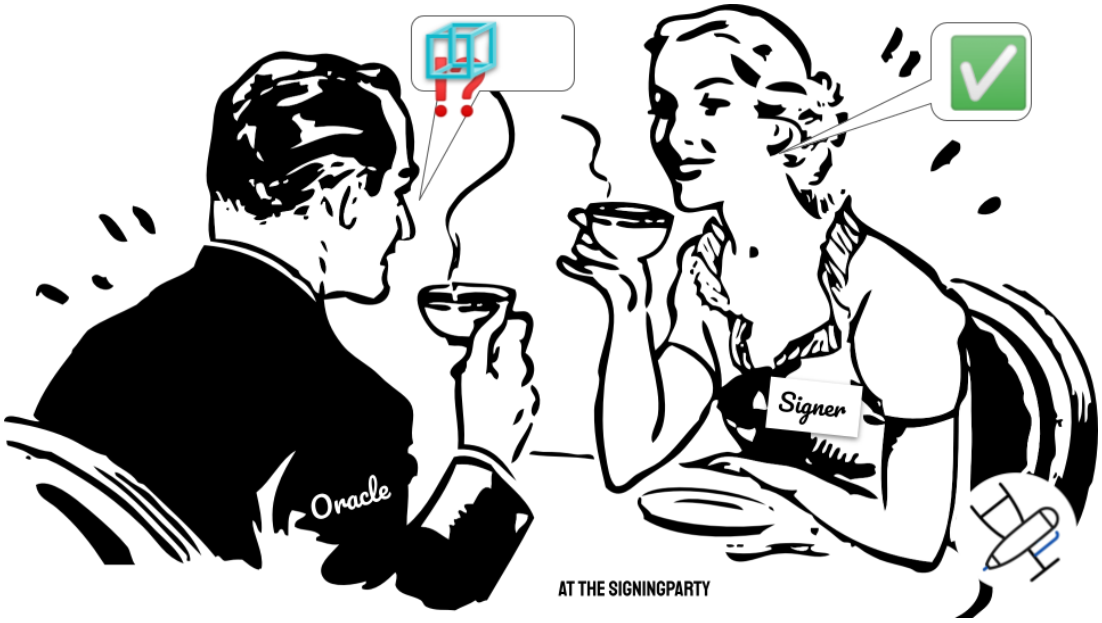
A web of trust enables an emergence of trust by cross validating the certificates of an increasing number of participants. As a result, if A trusts B and B trusts C, those direct line of trusts will be augmented by the implicitly created indirect line of trust between A and C.



We're kind of porting this approach to the web3 world of Real World Assets. Think on-chain trust, powered by the people.

The process

How does a signing party look like?



Does this thing exist as described?

1. A creator puts up a record to be signed
    - Defines the metadata the oracle will be asked to validate
2. An organizer (can be the same as creator) organizes a signing party to verify the record
    - A signing party is defined by time, place and record to be signed
3. He sends an invite with time and place
    - On chain and off chain
4. At the party, the signers answer the oracle questions
    - It's a reality check
5. The result: a probabilistic proof of existence
    - Comprised from: positive validations of oracle questions, scores of signers, creator, organizer

We the People

In a web3 world, we're all wallet addresses and their graphs. But for our social validation, the signers need to be unique humans. Otherwise, the setup will be prone to sybil attacks, where wallet bots pretending to be humans roam freely.

Soulbound Tokens

The Soulbound Token (SBT) adds a human layer to web3, with permanent, self sovereign IDs. Their interactions form a graph, which enriches wallet addresses with real world trustability.

The SBT may only exist as a proposal for now, but projects working on DID and SSI are quite plentiful. We really like the anti-sybil approach of Gitcoin's proofofpersonhood.com. But in its current state, PPOP is geared more towards dev related affairs.

For the time being, we will be sticking with BrightID, an ID chain based on Ethereum (and part of the proofofpersonhood scoring as well).

Just like Soulbound Tokens are not transferable, our signed NFTs have a permanent relationship with the underlying asset or object. So we may call them Objectbound Tokens.

Roles

Every unique person can have different roles in our setup.

The Creator

A creator has the power and the rights to create the canonical record of an object. The creator defines the meta data for the oracle questions.

A creator may want to extend his real life person and ID into the non-physical world by using his real name or his real world pseudonym (think: Banksy).

The Organizer

The organizer sets up the signingparty: which record to validate, which signers to invite and where to and when.

An organizer may want to extend his real life person and ID into the non-physical world by using his real name or his real world pseudonym (think: gallery name).

The Signers

The signers validate records by answering the oracle questions.

A signer may want to extend his real life person and ID into the non-physical world by using his real name or his real world pseudonym - or may decide to stay pseudonymous.

Friends and family

Your closest allies and supporters are central to your success. Of course you should invite them to sign off your works!

Unfortunately, usually their credibility outside of your circle only goes that far.

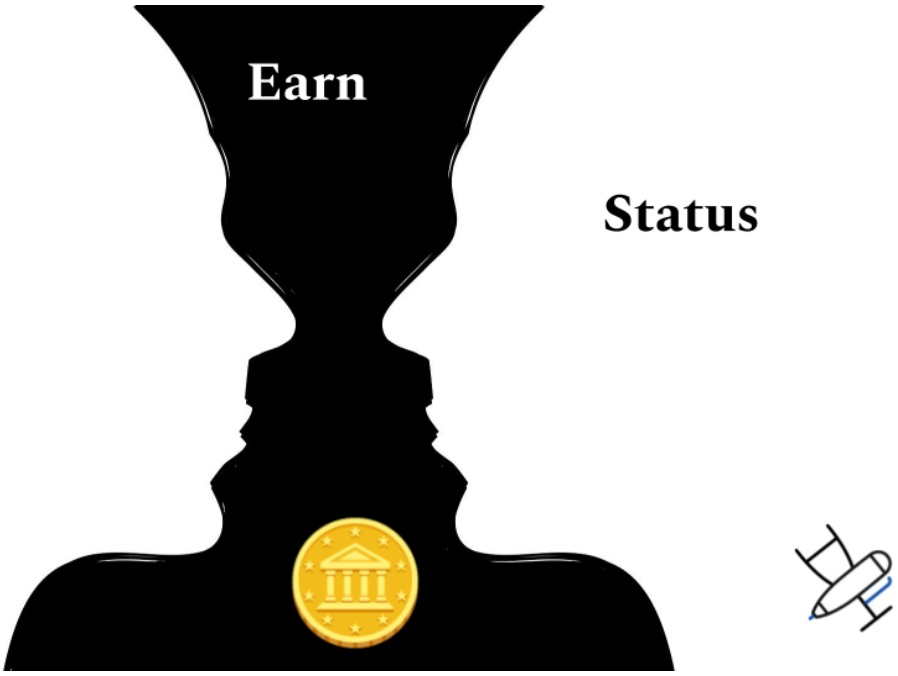
Guild of Signers

That's why there will be incentives to "upgrade" power signers into a Guild of Signers, whose members will act like trust boosters.

Guild members might be even able to add further credentials to their signer's profile, e.g. proof that they are specialists in certain areas.

What are the incentives?

The different roles may have slightly different incentives for their activities. As Li Jon wrote in Twitter: *The most successful web3 social apps are going to look completely different than web2 social (rather than building "decentralized Twitter/FB/X") They'll lean into financial speculation & create new economic status games.*



This fits very well into our proposed setup for creating an infrastructure for trust:

- it's a social network with a purpose
- it deeply interconnects with reality
- it's not an attention-grabbing stream like Twitter or Facebook, which are actually quite close to the linear TV experience of the 20th century

Fame

Actually, it should be fun and fame. Because a signing party is not just about the signing, but the party as well. It's a real life event for a few, hand selected people.

Over time, your profile will get populated with the party-NFTs and your sign offs. So the real life fame extends into the web3 world as well: what's your standing in the Guild of Signers?.

Earn

There will be a financial incentive to sign off records. But there need to be financial incentives for well behaved sign offs as well - and penalties for misbehavior.

Pay for Play needs to be discouraged - but at the same time, the signers will have to be incentivized. Accordingly, all fees are distributed across all active signers.

Signing Parties are actually collectable NFTs. Revenues coming from those sales are partially distributed across all signers as well.

The Trust Certificate

How will the rank in the web of trust be displayed?

1. The score is probabilistic
    1. The score is a snapshot in time
    2. The score relies on the score of the participants (creator, organizer, signers)
2. The calculation of the scores is subjective
    1. Different viewpoints may lead to differently weighted variables
    2. This relates mostly to the scores of the people involved

This means

- The signingparty DAO will create an implementation of the score.
    - the variables will be set by the DAO

- But based upon the same metadata, other implementations may come to totally different scores by coming up with different weights.

The Arts and other Areas of Application

We start with the arts, for various reasons. We have some relevant contacts into the world of arts, signing parties for NFTs sound like quite fun events and helping to clean up some clutter in the NFT space might be a worthwhile exercise anyway.

Examples of Other Areas of Application

Small Farms

Think small farmers certifying their organic farm, their food production or even batches of their delicious produce. Another route might be opening pathways for small scale agricultural carbon sequestration

Digital Twin Setups

If you're processing digital twins, you might want to "seal" your endpoints, like scanners, readers, gates or even the products themselves.

News

Yes, you could sign off news facts as well. Obviously so, the point of view of the signers and the applied lens will shape the outcome.

Example: think about an event in a war area. A drone has destroyed a car. You could assemble a small party to certify certain data points to the event. Depending

on the applied lens, the results will differ: e.g. a Russian lens on participating Ukrainian signers might paint them as biased.

DAO

A DAO will steer the development of the protocol and its first implementation.

SubDAOs

Area Specific Meta Data

The oracle will need a core set of meta data to be specified, which may be mandatory and specific for the vertical of application. For an art work you need different pointers than, let's say homemade organic jam.

The meta data fields will be set by sub DAOs.

Trust Certificate definitions

The core implementation of the scoring based on the graphs will be set by a sub DAO.

Conclusion

Real people connecting real things with web3.

Key Links

Website: https://signingparty.xyz

Twitter: twitter.com/SigningParty

Discord: https://discord.gg/cMdjYzs5