Trusted Crypto Asset

Proposal for a decentralized trust framework enabling the regulation of crypto assets in DeFi applications

The Hague - Rebooting the Web of Trust 11th
Belsy Yuen, Elena Chachkarova, Egidio Casati

NYMLAB

VectisDAO

See the paper repo

Join our discord

NGI ESSIF-LAB

Part of the work has been possible thanks to eSSIF-Lab - Business Oriented Call 1 (with project Gaya) and Infrastructure Oriented Call 1 (with project Verifiable Credential Authority

Trusted Crypto Asset Explained like i'm 5

NETWORKS

- Layers 1 and 2 are like road networks. They are public goods, commons in essence.
- Some of them look more secure than others, some smoother, some rougher, some faster or larger in capacity.
- Together they form an essential infrastructural network capable of moving [not people and goods but] value around

ASSETS

- Digital money, tokens in general are the medium that is used to standardise and transfer that value.
- similarly to cars, trains, planes that are the media to move people and goods around.
- There will be a very diversified offering of money, like

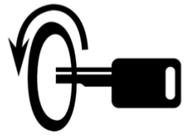
HOLDERS

- Users who want to use the distributed network and certain specific dApps, i.e. our drivers, will need to be licensed and recognisable at all times

Car checks driver when engine starts

- To drive certain vehicles on certain specific routes, drivers need to present proofs of specific requirements, such as driving license, special permits and authorisations.
- In the same way, a wallet holder will need to be able to present proofs of specific VCs in order to run specific dApps and enjoy specific products

- Drivers will interact with numerous regulated Issuers to request the Verifiable Credentials they need.
- Issuers, Verifiers, and users will be leveraging on the SSI protocols to issue/present/verify proofs in atomic way



- Crypto tokens are the vehicles that will require a systematic, upstream check.
- This will be obtained not by random cops going around checking driving licences or assessing a crime but by SSI-based present/proof and verify/revocation every time the engine is turned on

anyone can drive safely

- a new type of vehicle, designed to be easily driven, equipped with every comfort without the driver having to be an engineer
- similarly, crypto/identity wallets must be designed for mass adoption: no seed phrase, no gas friction, etc

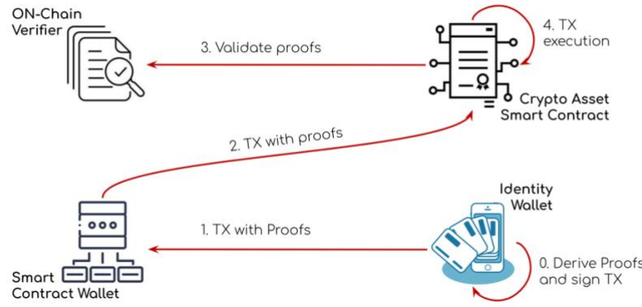
- the car, in order to be type-approved, must be equipped with appropriate safety measures, such as lane-change warning, anti-skid, etc.
- Average users approaching dApps must be provided with built-in consumer protection mechanisms, such as social key recovery / rotation, transaction limit / approval, auditability, etc.

- Roads, railways, ports and airports need to comply with safety, security and governance requirements. Specific Authorities oversight this
- Similarly, layers-1, layer-2, and smart contracts are infrastructural components of networks that deal with value and need to comply with security and governance requirements. Tokenomics introduces the concept of incentivised Market surveillance

Combining SSI with deFI

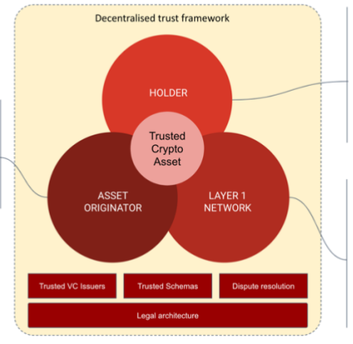
- dApps', smart contracts, minters of stablecoin and securities tokens will become the network's decentralised Verifiers: every time the user interacts with the smart contract, minting or negotiating a trusted crypto asset, the smart contract will validate the injected proofs and approve or block the transaction.
- This will promote a paradigm shifts from an intermediary-based system to an autonomous and privacy protected [proofs are ZK-ed and so can be kept on chain] SSI-based "present/proof, verify/revocation system.
- Two revolutionary features:
  - eligible users are verified seamlessly;
  - Verifiable Credentials and proofs remain in control of the users

TCA High Level Flow



Framework Overview

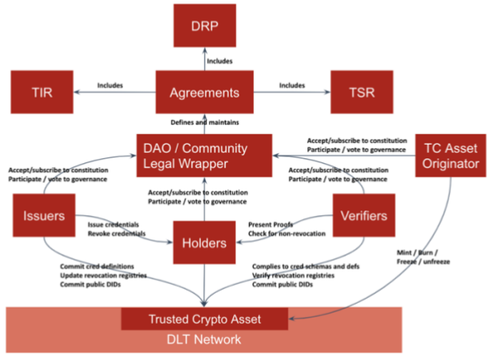
- Originator's Registered legal entity
- Policies
- Procedures
- Auditing of reserves
- Compliance to tech standards (i.e. erc20 / erc721 / erc1155 / etc.)



- KYC/AML verifiable credential holders (issued by a Trusted VC Issuer)
- Privacy preserving KYC and AML verifiable presentation / proof checks
- Verifiable presentation / proof non revocation
- Proof of using a certified wallet (eIDAS2)

- By analogy with eIDAS defined Qualified Trust Service Provider:
  - Registered Legal Entities
  - KYC and AML checks (by Trusted VC Issuers)
- Policies and procedures
- Further legal/org/capital requirements in case the network offered staking/delegation services

Legal Architecture



Technical Architecture