TPL: A Validation System for Secure Peer-to-Peer Exchange

Demian Brener
demian@zeppelin.solutions

Santiago Palladino
santiago@zeppelin.solutions

March 2018
WORKING DRAFT
https://tplprotocol.org

Abstract

Participants of an open economy can suffer from scams and immoral activities related to the issuance and exchange of digital assets. Government regulation provides part of the solution, but the main benefits are lost if a trusted third party is required to pass and enforce rules. We propose a solution to prevent malicious behavior by using a self-regulatory framework, elected by a peer-to-peer network and enforced on-chain. Participants in the network delegate trust to authorities for signing certificates and validating their identity in the network. The TPL protocol approves or rejects transactions according to certificate requirements that are coded into digital assets themselves. Any wallet, operating system or exchange (either traditional or decentralized) can automatically adhere to this protocol so that secure connections to other certified participants work seamlessly. In this way, TPL allows any project to guarantee regulatory compliance in every single exchange between participants, and not just in the initial offering.

1 Introduction

Clear guidelines for safe and reliable economic exchange are necessary to prevent malicious behavior within an economy. Scam organizations and theft could be disincentivized by impeding transactions that involve them or blocking electronic payments involving stolen funds. While government regulation works well enough for legacy economic exchange, it suffers from the inherent weakness of having a single party in control of passing, running and enforcing mandatory laws within a jurisdiction. In an inherently decentralized space, the emergence of centralized points of authority is likely to be antagonized.

Territorial-based jurisdictions lack a defined mapping to borderless cryptocurrency spaces. The result for the end user is a multiplicity of regulation sets, not necessarily compatible or consistent with each other, with no clear range of applicability and the uncertainty of change over time. In open exchange platforms, governments conduct their regulatory efforts via proxy - by regulating, auditing, suing and even banning [1] centralized exchanges and wallets that hold private keys [2], or projects selling tokens [3]. While aimed at protecting their citizens, tight control and dramatic penalties impose fear. This only ends up reducing the rate of innovation and wealth creation efforts within their jurisdiction.

What is needed is an open regulatory system that is governed by the network and enforced on-chain, allowing parties that trust one another to transact securely. A self-regulatory framework where participation is opt-in allows for the creation of multiple digital jurisdictions, each with its own set of rules, to appeal to different participants while balancing external legal requirements.

We propose an on-chain protocol for executing digital asset transactions within a peer-to-peer network of trusted participants. A formal decentralized economy creates strong network effects for participants to transact with trusted peers, rather than with participants that havent been validated or trusted.

2 Certificates and delegation of trust

We need a mechanism to ensure the adequate identification of participants according to the regulatory framework elected by the network. The solution we propose borrows from how trusted certificates are used in SSL (Secure Sockets Layer) [4], a protocol created by Netscape in 1994 and adopted by major web browsers to identify secure connections to a server via the Internet [5].

2.1 Root Authority DAO

Peer-to-peer networks can be regarded as virtual jurisdictions, not related to geopolitical boundaries, but to different sets of regulations and compliance guarantees. In it, we introduce the concept of a Root Authority DAO.

A Root Authority DAO is an entity that governs and manages rules within a jurisdiction. This Root Authority DAO elects Certificate Authorities to attest participants identity by signing certificates. Each set of Root Authority and its approved Certificate Authorities represent a jurisdiction with its own set of rules and processes.

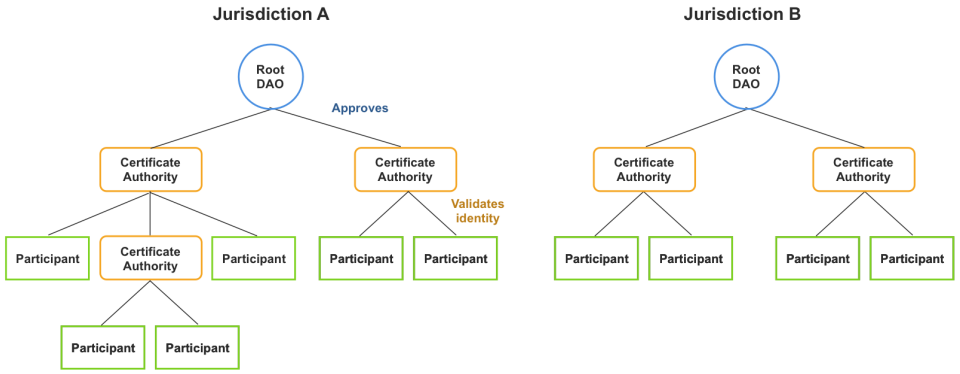

Figure 1: Delegation of trust between agents of specific jurisdictions, in this case, A and B.

A RootDAO promulgates industry guidelines governing the issuance and management of certificates within its jurisdiction, analogous to what happens in SSL with a CA/Browser Forum [6]. As a Decentralized Autonomous Organization, token holders govern a RootDAO following its preferred on-chain governance mechanism[1].

We expect successful RootDAOs to be set up as a consortium of respected exchanges, wallets, operating systems, and certification authorities. These will be trusted organizations from the blockchain space, who can watch over the end-users' interests and balance the legal requirements imposed. The open-source nature of RootDAOs allows for the creation of multiple jurisdictions to fulfill the needs of different networks.

2.2 Certificate Authority

A Certificate Authority is a trusted party that performs Know Your Customer (KYC) and Anti Money Laundry (AML) compliance due diligence and investor accreditation to participants in the network. The RootDAO approves and overlooks the performance of each CA and may oblige them to undergo regular security audits to ensure that they follow all process requirements. The RootDAO delegates its participants trust to CAs for issuing and signing certificates for end users.

[1] These may range from simple voting to token curated registries for managing lists of approved Certificate Authorities.

A CA can provide validation services to participants in exchange for a fee (e.g., Verisign [7]) or for free (e.g., Lets Encrypt [8]).

CAs may be subject to local governments influence, as they perform KYC-AML checks (or any other check required by the RootDAO) on the off-chain world. CAs have a strong incentive to balance local government pressure with guidelines from the RootDAO, as it can remove a CA from its trusted set if it deviates from its requirements, instantly revoking all end-user certificates emitted by the entity.

We expect prominent projects within the blockchain space to act as CAs themselves to vouch for their users as part of their service offering. Other projects may fall back to generic CAs who provide such service in exchange for a fee. Additionally, ICO platforms such as Coinlist already perform KYC-AML due diligence and investor accreditation and thus could act as CAs.

2.3 Participant

A participant is any individual or entity that wants to transact within a trusted network. Participants rely on certificates to transact with other trusted members. They gain access to these certificates in exchange for sharing their personal data with CAs via KYC-AML procedures. These certificates are valid for a period, after which participants must renew them via CAs.

Participation in a jurisdiction is not exclusive. Participants may have certificates from multiple jurisdictions, should they wish to take part in exchanges in networks with varying requirements.

We expect that the majority of wallets (e.g., MyCryptoWallet), exchanges (e.g., 0x) and operating systems (e.g., ZeppelinOS) will support certificates from various RootDAOs so that the certificate chain can be validated efficiently, and safe connections to other certified participants work seamlessly.

3 Certificate issuance

A CA can use a combination of authentication techniques to validate the identity and accreditation of participants. These include leveraging government bureaus, the payment infrastructure, third parties' databases and services, and custom heuristics.

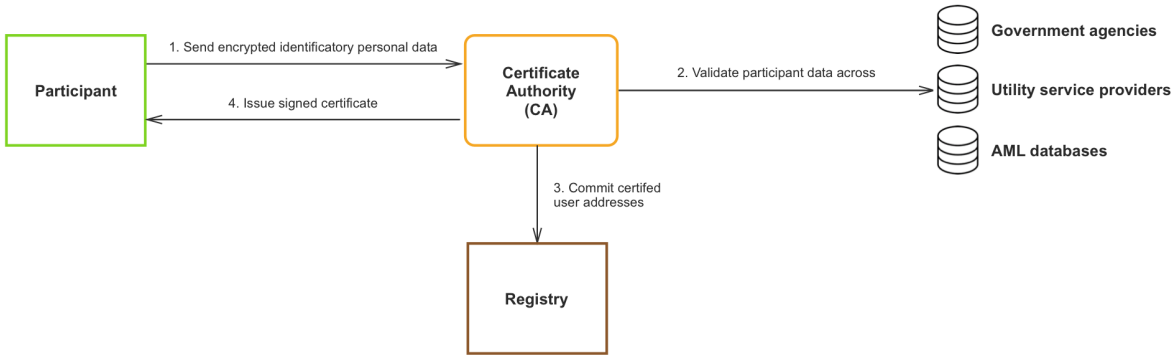

Figure 2: Validation and certification process.

A CA-issued certificate can include multiple extensions that act as different level authorizations or usage scopes. In the case of an ICO, a project can adhere to a specific jurisdiction, and require participants to hold certificates asserting their accredited investor status and their ability to operate under a particular countrys law[2]. Additionally, different certificate extensions could allow for up to a specific volume of

[2] For privacy concerns, the certificate could be used for KYC-AML purposes only without revealing participants identity

transactions.

4 Potential implementations

Certificates in TPL are analogous to X.509 certificates [9], allowing for the re-use of existing tools and libraries to generate and sign certificates.

A RootDAO signs certificates for the CAs with its private key. CAs then sign the corresponding participants' certificates. When a participant wants to prove that they belong to a jurisdiction, they present the certificate chain up to the RootDAO certificate.

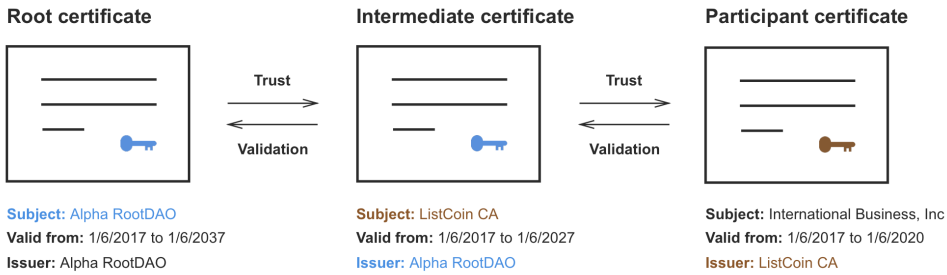

Figure 3: Validation and certification process.

A RootDAO governs a smart contract on the Ethereum [10] blockchain that mirrors the chain of trust of certificates. This smart contract-based registry allows any smart contract to easily check that a participant is indeed part of the jurisdiction by querying this on-chain registry, rather than cryptographically verifying the authenticity of the certificate chain. Additionally, having all certificate info in a single smart contract facilitates certificate revocation[3].

4.1 Approval of transactions between trusted participants within a jurisdiction

The logic for transaction approval can be automated and built-in within the smart contract code of a token or an exchange. TPL can enforce any compliance rule required by a project sponsoring an asset, assuring that all participants in a transaction have been adequately vetted.

This mechanism allows any project to ensure that not only their ICO will be compliant, but also any subsequent transactions of their asset between any third parties since the contract itself can reject any operations from unauthorized users. Different token contracts may demand various extensions to be present from the transaction participants certificates, thus effectively placing on-chain any off-chain compliance requirements. Any vendor (wallet, operating system or exchange, either traditional or decentralized) will automatically adhere to these requirements since they are coded into the digital asset itself.

Alternatively, if TPL is not built-in within an asset smart contract code, any vendor can still protect its end users by querying participants certificate identities within the jurisdiction public registry.

5 Next steps

Blockchain technology empowers the individual, holding the promise of an open financial system. While it has steadily matured over the last few years, significant challenges remain, in particular towards inte-

[3] This outperforms protocols like CRLs or OCSP

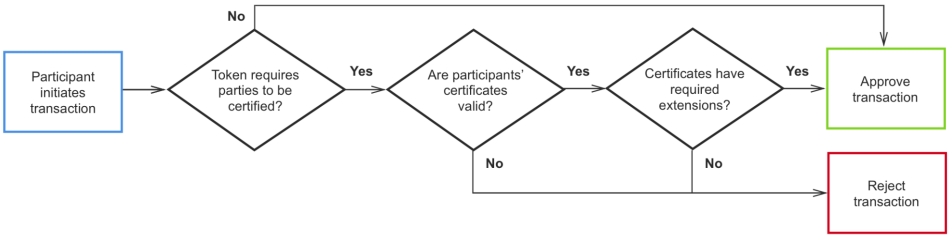

Figure 4: Validation and certification process.

gration with the traditional financial system. If performed wisely, this integration could lead to a new world in which the usual power relations are inverted, and individuals are in control.

This process, however, might be at risk if driven from outside the system as institutions will naturally favor the status quo. To be successful, the integration must be led from within, proposing clear guidelines on how to onboard institutional players. TPL is a first approach in this direction, providing a self-regulatory framework to support formal decentralized economies while preserving users freedom to assemble and innovate.

Should this idea find consensus among the community, we will include support for permissioned tokens within OpenZeppelin [11], a standard framework of reusable and secure smart contracts in the Solidity language.

References

[1] Xie Yu. China to stamp out cryptocurrency trading completely with ban on foreign platforms. http://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban. Accessed: 2018-03-26.

[2] Coinbase Support: Identity Verification. https://support.coinbase.com/customer/portal/articles/1220621. Accessed: 2018-03-26.

[3] Alex Wu. Tutorials for the 0x Token Sale Registration . https://blog.0xproject.com/tutorials-for-the-0x-token-sale-registration-766064955d12. Accessed: 2018-03-26.

[4] What is an SSL Certificate and How Does it Work? https://www.digicert.com/ssl/. Accessed: 2018-03-26.

[5] History of SSL Certificate. https://www.evsslcertificate.com/ssl/ssl-history.html. Accessed: 2018-03-26.

[6] CA Browser Forum. https://cabforum.org/. Accessed: 2018-03-26.

[7] Verisign. https://verisign.com/. Accessed: 2018-03-26.

[8] Let's Encrypt. https://letsencrypt.org/. Accessed: 2018-03-26.

[9] X.509 Certificate. http://searchsecurity.techtarget.com/definition/X509-certificate. Accessed: 2018-03-26.

[10] Ethereum Project. https://ethereum.org/. Accessed: 2018-03-26.

[11] OpenZeppelin. https://openzeppelin.org/. Accessed: 2018-03-26.