0xcert protocol

Open protocol for certified non-fungible tokens

Version 0.11
Authors: Kristijan Sedlak, Jure Zih
0xcert.org

Abstract

0xcert is an open source, permission-less protocol for certified non-fungible tokens on the blockchain. These tokens are stored in cryptographic wallets and are owned by users. In addition to common functions for managing and transferring standard non-fungible tokens, the 0xcert protocol provides conventions for creating certified non-fungible tokens from unique digital assets. These tokens are called Xcerts and are created through a custom minting process. Xcerts represent standard non-fungible tokens, which also hold information about a real-world digital asset. With 0xcert protocol, we can validate a proof of existence, authenticity, and ownership of these digital assets without third-party involvement.

0xcert is a framework with a set of on-chain and off-chain rules for managing Xcerts and other standard non-fungible tokens. Our mission is to equip application developers with a secure blockchain settlement, powerful tools, and community embraced conventions for managing non-fungible tokens. 0xcert is a pluggable settlement with an advanced integration layer for different dapps and relay applications. This enables developers to focus on the application layer and quickly build applications for issuing university certificates, KYC applications, applications for loyalty programs, warranties, badges, credits or even a decentralized non-fungible exchange.

0xcert also provides and manages an online 0xcert Explorer dapp, which enables a live view of the 0xcert network, together with interfaces for interacting with the protocol.

Contents

1. Introduction

0xcert is an open source, permission-less protocol for certified non-fungible tokens on the blockchain. These tokens are stored in cryptographic wallets and are owned by users. In addition to various common functions for managing and transferring standard non-fungible tokens, the 0xcert protocol provides conventions for creating certified non-fungible tokens from unique digital assets. These tokens are called Xcerts and are created through a custom minting process.

Xcerts represent standard non-fungible tokens, which also hold information about some real-world digital assets. With 0xcert protocol, we can further validate a proof of existence, authenticity, and ownership of these digital assets without third-party involvement.

The first implementation of the 0xcert protocol is focusing on the Ethereum blockchain. Because the 0xcert protocol tries to be blockchain agnostic, we would like to support other blockchains as well.

1.1 Overview

Our mission is to equip application developers with a secure blockchain settlement, powerful tools and community embraced conventions for managing non-fungible tokens. 0xcert protocol extends the non-fungible paradigm with a unified certification layer for unique digital assets based on 0xcert conventions. This allows for creating certified non-fungible tokens, which carry information of a unique real-world digital asset.

The protocol supports a wide range of use cases, where digital assets and ownership play a role. Because the data are stored in decentralized blocks, the information can fully be trusted and verified by anyone and anywhere.

It provides a unified blockchain based certification layer for unique digital assets, which eliminates the need for a middleman between parties involved in the process. Anyone can use the fully functional 0xcert protocol completely free of charge, with the ability to manually mint, burn, verify and transfer Xcerts. In

addition, the protocol uses a publicly accessible network of digital wallets and smart contracts, making it extensible through third-party modules and a variety of dapps on a shared infrastructure.

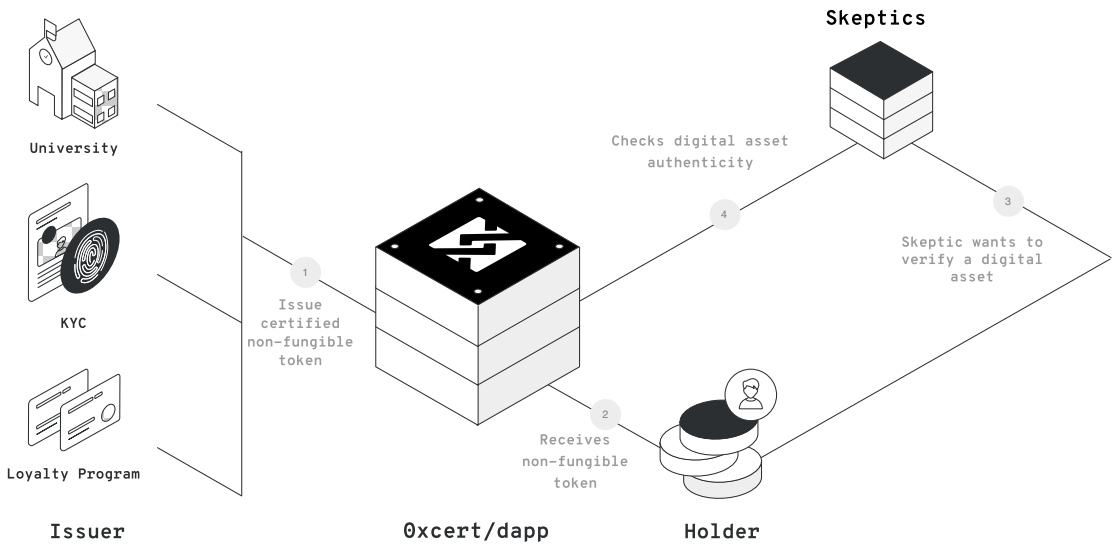

Figure 1: 0xcert protocol can act as an intermediary between issuers, holders, and skeptics.

0xcert is an opinionated framework and supports numerous business models used by third-party dapps. These applications sit on top of the protocol and can use XCT tokens as a fuel for their services. The dapps form a network of public and private unique digital asset certification services and offer higher-level features that simplify and automate the certification process, provide public and private listings, rewarding mechanisms, integration gateways and more.

1.2 Fungibility

The most common tokens of today's crypto economy follow the Ethereum's ERC-20 specification. These tokens carry a price, which can be divided into smaller amounts. One can exchange just a portion of that price for a service or for different tokens. This is called fungibility, thus these are called fungible tokens.

Recently, another kind of token called non-fungible tokens started getting attention in the crypto community. It all started with Cryptokitties - tradable collectibles - which set the foundation for the now accepted ERC-721 standard. Unlike ERC-20 identical tokens, which carry a price, non-fungible tokens are unique and carry some sort of data.

The 0xcert protocol introduces an Xcert as a certified, non-fungible token based on 0xcert conventions, and it carries information about a particular digital asset. This mechanism is unique to the 0xcert protocol and is described in later sections.

Fungible tokens

Non-fungible tokens

Xcert

1.3 Decentralization

Certification represents compliance with specific requirements. It can cover products and their components, services, people, and systems.

Digitalization of different assets has already introduced a new way of storing and sharing information online, making certification cheaper and more convenient for all involved parties. However, the ability to easily copy and share this data, also makes it vulnerable to various exploits, hacks, and falsifications.

The protocol utilizes the blockchain, a distributed ledger technology that was first built to support the Bitcoin cryptocurrency. Blockchain can be best described as a distributed ledger that maintains a list of records called blocks. Each block has a timestamp and is built on top of an already existing block, preventing any data from being altered retroactively.

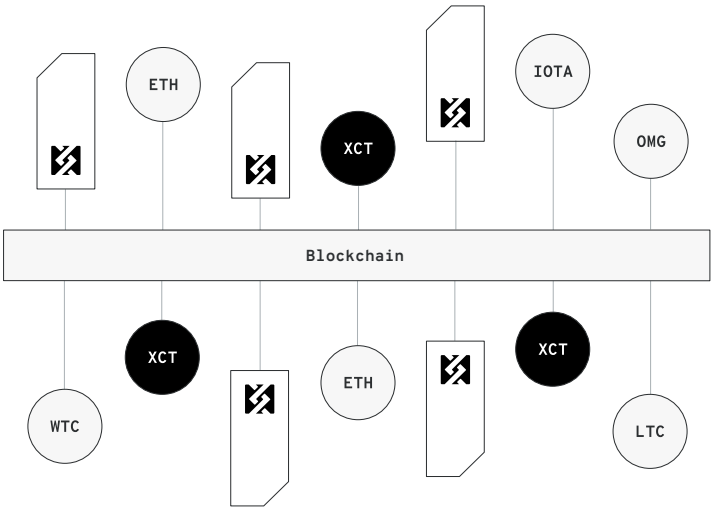

Figure 2: 0xcert protocol uses blockchain to store digital asset information.

Blockchain offers a unique solution to the problem of secure online transactions. Due to its transparency and distribution of information to many decentralized blockchain nodes, it is nearly impossible to manipulate existing data records, making it potentially suitable for recording events, records, identities, certificates, transactions and other documentation.

Certification can benefit greatly from this new paradigm. By storing hashed data on the blockchain, individuals, companies, and institutions can keep a decentralized record of their certificate proofs, while maintaining sensitive data completely private. At the same time, all certificate records, their issuers, and owners, can be easily authenticated and referenced.

2. Specification

0xcert provides a framework with a set of on-chain and off-chain rules for managing Xcerts and other standard non-fungible tokens. It is a pluggable settlement with an advanced integration layer for different dapps and relay applications.

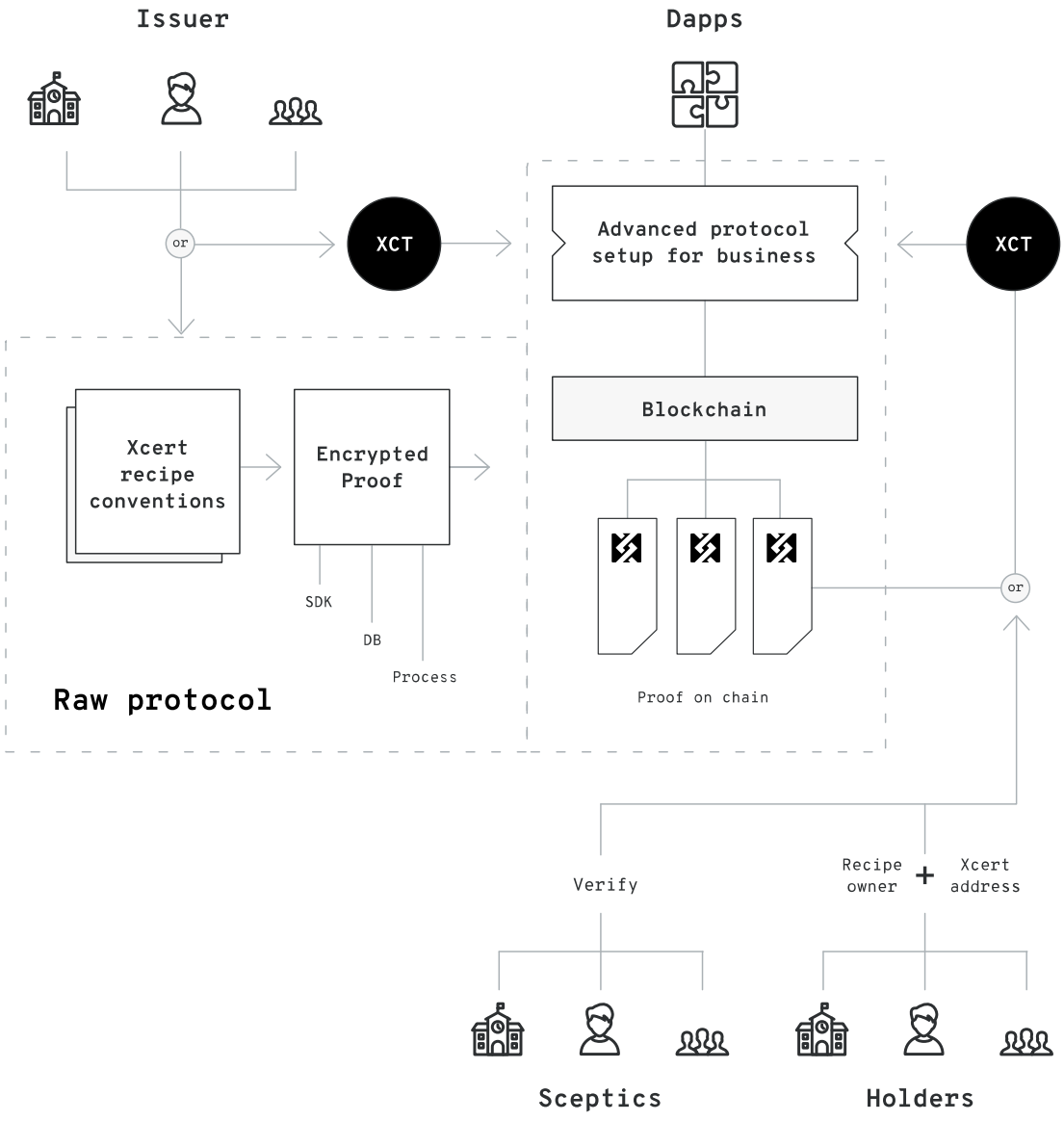

Figure 3: Users can interact with the protocol manually or through higher-level dapps.

2.1. Xcert

According to William Mougayar, author of "The business blockchain", a token is "a unit of value that an organization creates to self-govern its business model, and empower its users to interact with its products, while facilitating the distribution and sharing of rewards and benefits to all of its stakeholders."

An Xcert smart contract is a standard non-fungible token smart contract. Similar to well known ERC-20 token contract the Xcert smart contract is a specifically designed smart contract, which follows the Ethereum's ERC-721 specification also known as a deed standard.

In its nature, as a non-fungible token contract, every minted Xcert (an item) is unique, unlike the identical ERC-20 token. Accordingly, Xcert can be a medium to any data or digital asset.

An Xcert carries an imprint of a unique real-world digital asset. The imprint is generated as a part of the 0xcert certification process at the mint time. It represents a cryptographic hash of a digital asset and serves as a decentralized proof of a digital asset on the blockchain. This makes the 0xcert protocol unique and extends the usability to a whole new level.

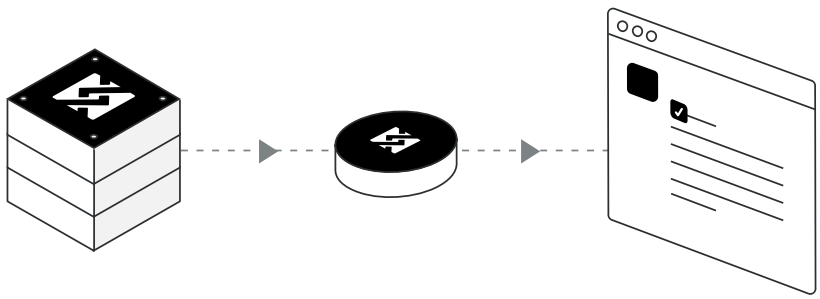

Figure 4: Xcerts are non-fungible digital assets that carry distinguishable data.

It is identified with an ID, it has an URI that points to the public JSON metadata file and holds an imprint of a real-world digital asset. An Xcert does not include actual asset data, only the proof of it. This ensures data confidentiality because no information is disclosed to the general public and the actual content is always kept private to the involved parties only.

2.2. Conventions

A digital asset in the 0xcert protocol is defined and described in the form of a specifically designed JSON object, which conforms to RFC-7159 and follows the mapping format defined by the JSON Schema specification.

The 0xcert protocol can cover all sorts of digital assets. A simple imaginary schema, that describes a person, could look something like this:

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "id": "https://specs.0xcert.org/schemas/person.json",
  "description": "A person (alive or fictional).",
  "properties": {
    "name": {
      "descripton": "A full name of a Person.",
      "type": "string"
    }
  },
  "proof": ["name"],
  "meta": [],
  "required": ["name"],
  "title": "Person",
  "type": "object"
}
```

Figure 6: Xcert schemas describe digital assets in a way that machines can understand.

Every digital asset in the 0xcert protocol has its own JSON Schema definition. The schema represents a technical specification of a particular digital asset. It explains the JSON object structure, validation and each property details.

The naming of JSON properties must follow the schema.org specification when possible. This is to enable an easy way to convert a digital asset data object into JSON-LD format. The convention also expects the JSON keys to be defined in alphabetical order. 0xcert protocol extends the JSON Schema specification and allows also to specify a list of fields that describe a proof and a list of fields representing metadata.

Schema documents are defined and approved by the interested community engaging the protocol. The community can propose updates and new conventions, which can then be included in the protocol, based on the majority consensus.

2.3. Certification

The minting process of a new Xcert is called certification. The result is a new certified non-fungible Xcert token. Xcerts are assigned to digital wallets and the ownership of each Xcert is immediately transferable among them.

New Xcerts can be minted by the issuer, who owns the Xcert smart contract or minted by an entity authorized by the issuer. The issuer can immediately transfer a new Xcert to a holder who then becomes the owner. Similar logic applies to the burning process, where the holder is also allowed to burn any Xcert that he owns.

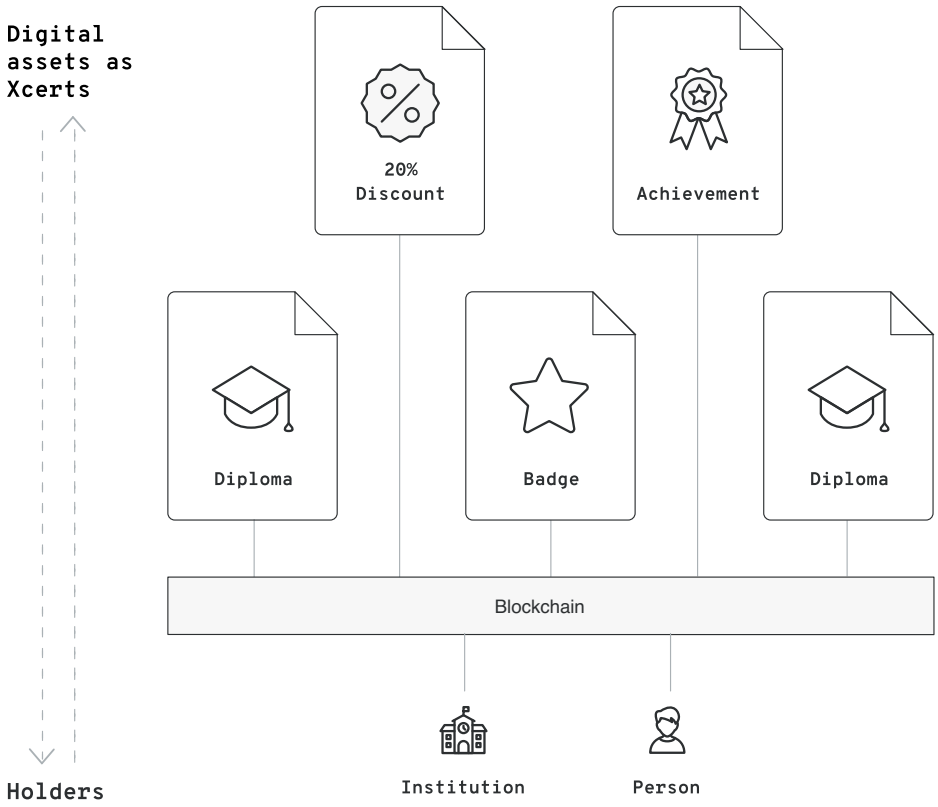

Figure 7: Xcerts hold information about different digital assets and ownership.

The manual certification flow is carried out in multiple steps, usually between an issuer and a holder.

An issuer represents a trusted authority that provides a value for the interested public. The issuer uses Xcerts on the blockchain to provide a proof of ownership for its digitized assets.

The issuer creates a new Xcert smart contract and deploys it to the public blockchain. This makes the issuer also the owner of this smart contract, with an ability to mint new Xcerts and transfer ownership to holders.

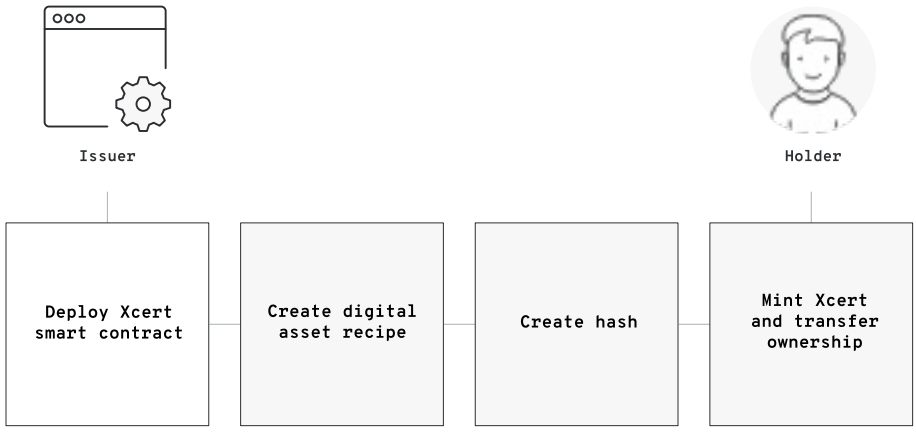

Figure 8: An issuer enables certification by deploying the Xcert smart contract to the blockchain.

The minting process of a new Xcert starts by creating a JSON object with information about a digital asset. As explained earlier in the document, this object holds information about a particular digital asset and can include product-related data, issuer details, holder identity information and more. The protocol provides a convention for each digital asset and specifies a list of required and optional keys, related type information and usage details.

When the JSON object is created, issuer converts it into a cryptographic hash, which is an imprint of a digital asset and represents a proof. The protocol allows different cryptographic algorithms to be used and it is up to the issuer to decide the appropriate level of security.

For the final step in the certification process, the issuer submits the cryptographic hash, together with holder's wallet address to the Xcert smart contract on the blockchain.

The minting process creates a new Xcert and assigns the ownership to the provided holder. When the certification is completed, the issuer sends the JSON data object over an arbitrary communication medium to the holder, so he will be able to provide the proof of ownership for the particular digital asset or burn it at his discretion.

All parties involved in the certification process are expected to keep a copy of the JSON data object, in the same way as they keep a copy of their digital wallet credentials. They can store this information locally or can authorize third-party dapps to do that on their behalf.

In terms of trust, the issuer is responsible to prove and promote their account authenticity information over arbitrary communication media when needed.

2.4. Verification

0xcert protocol allows for trustless verification of any kind of digital asset existence and related ownership. Anyone is able to verify some information based on digital asset imprint - the cryptographic proof - stored inside Xcerts on the blockchain.

In order to obtain valid information about a particular digital asset, a holder must disclose information to the skeptical party, and send the explicit JSON data object for the requested asset, through an arbitrary communication medium. A holder must also provide the appropriate Xcert smart contract address on the blockchain, where the digital asset imprint exists and can thus be verified.

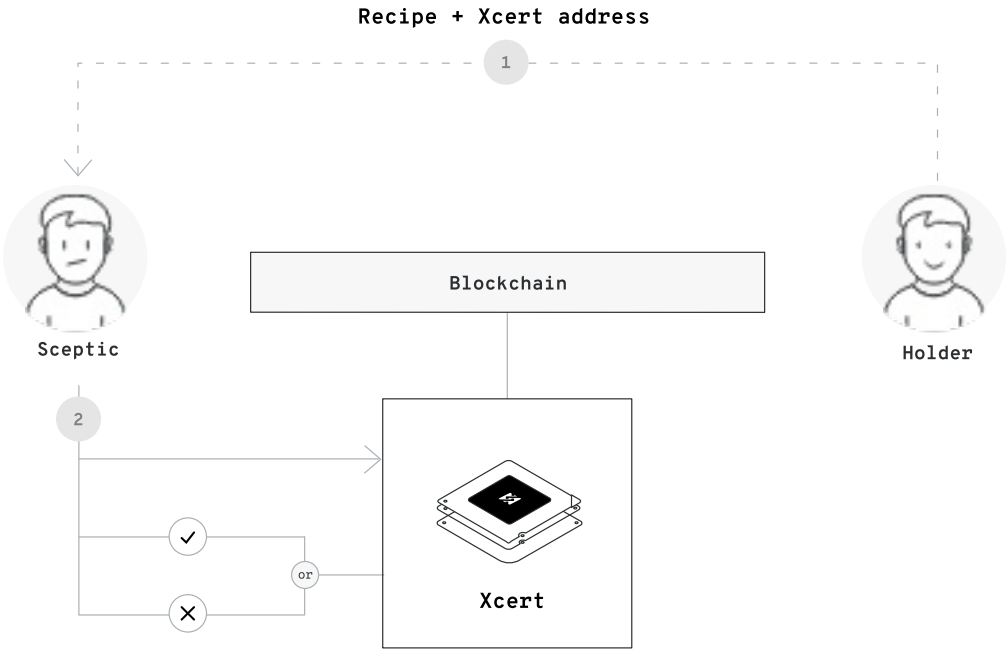

Figure 9: Xcerts carry a trustless proof of digital asset existence and ownership.

Based on the data received from a holder, the party creates a cryptographic hash from the provided JSON data object and then verifies that it matches with the one stored in the provided Xcert on the blockchain. When the hash strings are equal the information can be treated as valid and the holder can be trusted.

In terms of dapps, the verification process is usually automated. Some dapps might expect a holder to have the Xcert stored in his digital wallet. Holders are able to have all Xcerts stored in their digital wallets and share the proof of ownership with anyone at will. This enables a third-party to quickly and easily verify any provided information without unnecessary interaction.

3. Business layer

0xcert is a pluggable settlement with an advanced integration layer for different dapps and relay applications. In addition, the 0xcert protocol represents a low-level certification layer and defines the steps for different certification flows, strengthened by the conventions. The protocol allows for building higher-level applications and services, to enable advanced non-fungible features, usage simplifications, and automatization.

3.1. Third-party services

In addition to the raw protocol, 0xcert provides a set of smart contracts installed on the blockchain, with supporting SDKs, which cover different business models. This allows easy integration of the 0xcert protocol into existing systems.

Relay applications and other dapps don't have to struggle with the low-level blockchain complexity and can thus immediately start using a solid, secure and flexible non-fungible infrastructure that ensures interoperability between dapps by default.

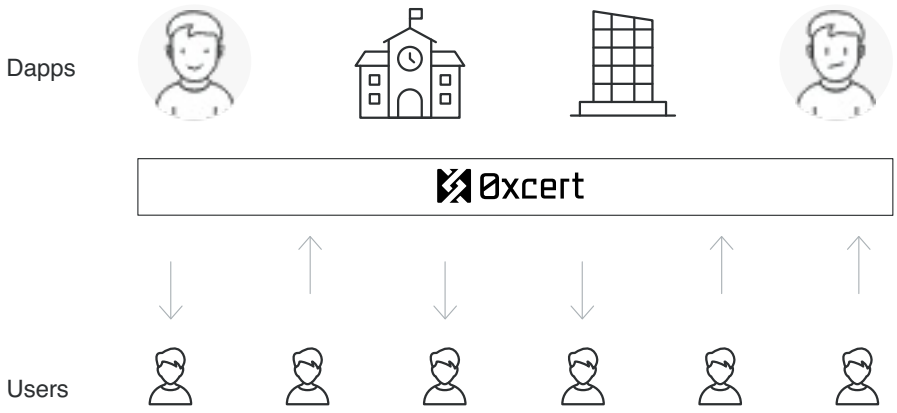

Figure 10: Applications on top of the 0xcert protocol form a network of non-fungible services.

This setup supports common business logic and serves as a decentralized proxy for handling communication between services and certification parties. Applications can use the protocol's XCT token, for payments or as a fuel for their services.

3.2. Protocol token (XCT)

XCT tokens are the native utility tokens of the 0xcert protocol. They are compliant with the ERC-20 standard contract ABI for tokens on the Ethereum blockchain.

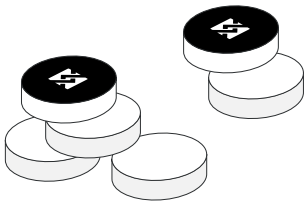

Figure 11: XCT tokens are native ERC-20 utility tokens and are used for paying fees.

XCT represents a protocol token - a utility token - and is introduced to align certification parties with dapps and assures that the proposed protocol can be adhered to.

With the infrastructure built around a system of smart contracts and dapps, its primary role is to provide the incentive mechanisms and support the ecosystem with minimum possible fees. XCT is the basic liquid asset for dapps that operate on the protocol, and similar to gas on the Ethereum blockchain it covers fees for issuing and verifying Xcerts.

3.3. Continuous integration

A smart contract cannot be changed after it is deployed to the blockchain. Changes can be applied only by deploying a new contract at a new address.

The protocol may include a decentralized governance (DAO) mechanism to allow the community to vote for improvements and possibly fork the protocol into multiple versions. The contracts may use protocol tokens to securely drive a decentralized continuous integration of updates with no disruption, while also protecting all the parties and stakeholders.

4. 0xcert explorer

The purpose of the 0xcert company, as the core team behind the 0xcert protocol, is to provide a foundation for trustless, certified, non-fungible tokens on the blockchain and to unify the community as much as possible. The company tends to bring value to the open-source community engaged with the 0xcert protocol, to connect individuals and groups working in the area of non-fungibility or certification, and to provide resources and support for the related community driven incentives.

In addition to the protocol itself, the 0xcert company provides and manages an online 0xcert Explorer dapp, which enables a live view of the 0xcert network, together with interfaces for interacting with the protocol, which represents the central hub for non-fungible tokens on the blockchain.

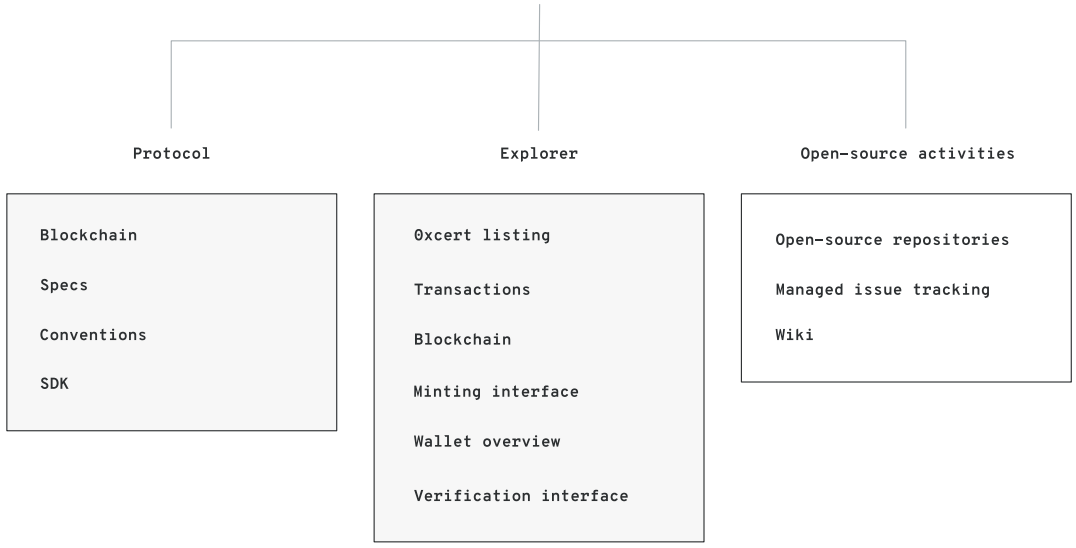

Figure 12: 0xcert Explorer is an open-source dapp, which includes a block explorer, search, API interfaces, W3C DID resolver and analytics for decentralized Xcerts on the blockchain.

5. References

Non-fungible Token Standard,
https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

Decentralized Identifiers (DIDs),
https://w3c-ccg.github.io/did-spec/

JSON Schema,
http://json-schema.org

Permanent Identifiers for the Web,
https://w3id.org

Structured Data,
https://developers.google.com/search/docs/guides/intro-structured-data

JSON for Linking Data,
https://json-ld.org/

JSON-LD Best Practices,
https://json-ld.org/spec/latest/json-ld-api-best-practices/

JavaScript Object Notation or JSON,
https://en.wikipedia.org/wiki/JSON

0x project,
https://0xproject.com

Blockcerts,
https://www.blockcerts.org

Open Badges,
https://www.imsglobal.org/sites/default/files/Badges/OBv2p0/index.html

MIT Media Lab Digital Certificates,
https://certs.media.mit.edu/