Blocksquare Inc.
Medius Inc.

Proof of Title (PoT)

25th September 2017, Version 1.0

Denis Petrovcic, Viktor Brajak

Summary

With Ethereum and the underlying technical merger of blockchain technology and coded objects, the idea of tokenizing real world assets has become reality. Transferring real world value over the internet poses the need to introduce a system to securely link these coded objects, referred to as smart contracts, to the cumbersome and archaic structures of various national land registries.

Ethereum smart contracts are programs run on a blockchain, with unique attributes compared to other forms of software. The program itself is recorded *on* the blockchain, which gives it characteristics like permanence, censorship resistance and irreversibility. This in terms means any line written in the smart contract will always be present and can not be modified at a later stage. Blocksquare makes use of these characteristics by copying property specific information from land registries and including it in PropToken smart contracts. On the land registry side, a note containing the PropToken smart contract hash address is added to the title deed. Where land registry data is accessible online, the Proof of Title protocol periodically reads this information in the PropToken smart contract and compares it with information pulled from a trusted source such as the land registry. An external oracle service provider is used to ensure auditable guarantee and connect the outside world with a decentralized application on the blockchain.

Note: the contents of this technical paper are subject to change.

“The problem with quotes on the internet is
that it’s hard to verify their authenticity.”

—Abraham Lincoln

Trust, verification and security.

Trust is one of the biggest issues on the internet. According to Mayer et al. (1995)[1] trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." Trust is something that has been seen as important when it comes to communicating, building relationships or exchanging value (Fukuyama, 1995)[2].

The blockchain introduces a trustless environment for online value exchange, but even so, users of the various blockchain networks and platforms put themselves at risk as the internet is uncertain and includes various types of unknown players. In Blocksquare's case, users of the network must trust that each PropToken smart contract in the Blocksquare network indeed represents the stated real estate property. Furthermore, PropToken owners must trust that the company providing the escrow services to hold legal title will not transfer the property title *off chain*. To induce trust and achieve no bad actors game the Blocksquare system, a secure method of verification must be introduced.

A trustless ownership verification protocol.

With land registries being accessible online in most countries, verified real estate ownership information is provided to the public by a trusted government source. This data is updated and maintained regularly by a trusted 3rd party - the government. If the property ownership information from this data source is copied to a PropToken smart contract deployed on the Ethereum network, the PropToken becomes irreversibly 'marked' as *the* smart contract representing the specified real estate property. We now have 1) a trusted government issued source and 2) a time-stamped smart contract containing the exact same information. A security verification protocol to periodically check the two records match can now be introduced.

[1] Roger C. Mayer, James H. Davis and F. David Schoorman., (1995). The Academy of Management Review Vol. 20, No. 3 (July), pp. 709-734.
[2] Fukuyama, F. (1995). Trust: Social Virtues and the Creation of Prosperity. NY: FreePress.

Land registry systems.

Real estate and many other assets that are costly to trade will be tokenized in the future[3] **only if the systems of tokenized assets provide enough trust to the general public**.

Today we trust in land registries that hold property and land ownership information. Land registries guarantee title to registered estates and interests in land by holding the proof of ownership and offering an easy-to-read document reflecting the contents of all the paper title deeds. All title information is kept in a central database where it can be usually viewed quickly and securely online.

As mentioned above there are positive elements to traditional land registry systems, but they also come with certain limitations. Obviously, they are all centrally owned thus slow and expensive to work with, they are definitely not adapted to latest technological advances (e.g. tokenized assets), they are cumbersome when managing shared property ownership, etc.

Eventually, market demand will dictate the transformation of land registry systems. Only time will tell whether the change will be towards decentralized applications (dApps), that do not rely on a single trusted third party. Although it is expected that some process will be kept off-chain, e.g. land parcelling, assigning land and building IDs, court dispute resolutions that change property ownership, etc., we can already witness advancements towards blockchain — for example Sweden setting up a blockchain based land registry.[4]

But before such land registers become reality we need to find a way to connect tokenized real estate to existing land registers.

Connecting tokenized real estate to the real world.

The main purpose of the Proof of Title protocol is to provide a trustless verification method to the network of tokenized real estate as proposed and currently being developed by Blocksquare (blocksquare.io). Blocksquare is not only developing the needed network infrastructure for real estate property tokenization, but also a platform to buy, sell and trade real estate tokens.

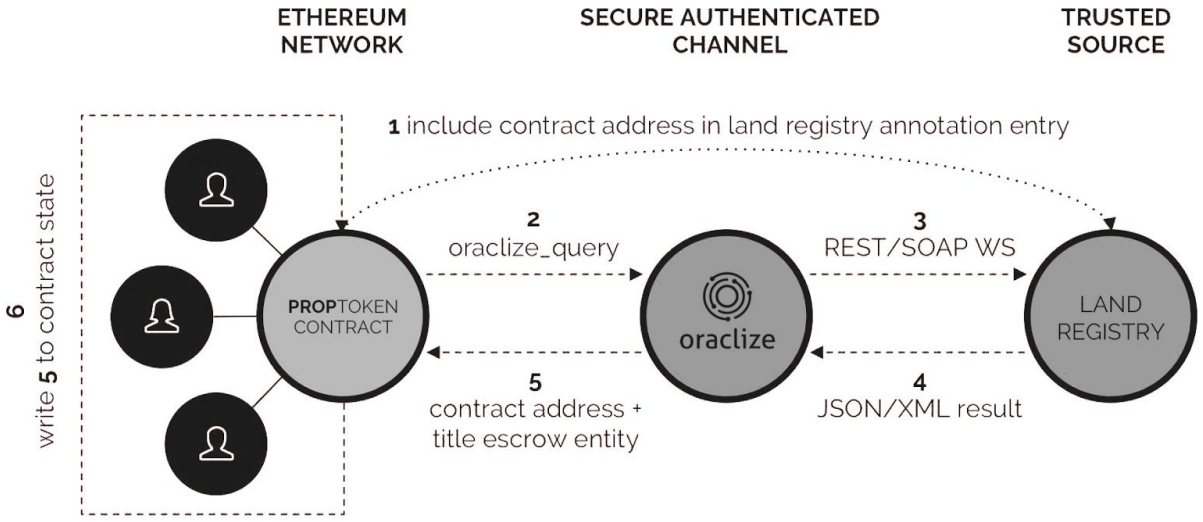
Each real estate property on the Blocksquare network is represented by a PropToken smart contract deployed on the Ethereum network. Properties added to the network are made available for users on the Blocksquare platform through a PropToken crowd sale process that mints and distributes PropTokens to participants. Although PropTokens give certain property rights to holders (e.g. simplified governance rights, property usage rights), the

[3] McKeon, S. (2017). Traditional Asset Tokenization. Source: https://hackernoon.com/traditional-asset-tokenization-b8a59585a7e0
[4] ChromaWay. (2017). Blockchain and Future House Purchases. Source: https://chromaway.com/landregistry

whole structure of accounts on the blockchain can not be reflected in traditional land registries.

To overcome this limitation, property titles are held by Blocksquare Foundation serving as a title escrow agent and trusted party. A copy of this title information from the land registry is also held in the tamper proof environment of the PropToken smart contract, whereas the Proof of Title protocol makes sure both ends reflect the same information, providing a trustless link between each PropToken contract and land registry title, effectively increasing trust among PropToken holders. Further on, an extended validation certificate is used to prove that Blocksquare Foundation is also the issuer of all associated PropToken contracts.

Proof of Title (PoT) Schematics.



How Proof of Title (PoT) works?

Today we trust in land registries that hold property and land ownership information. To explain how Proof of Title works we will use a practical example from the tests conducted in Slovenia. For explanatory purposes you may refer to the paper Legal Framework in Slovenia - OeNB (p. 33-39)

The Slovenian land register[5] is owned and managed by the Supreme Court of the Republic of Slovenia and offers the ability to access data such as cadastral municipality, parcel number, building number, individual part number, property ID and right ID.

Nepremičnina

tip nepremičnine: 1 - zemljiška parcela
vir ID znaka: 1 - zemljiški kataster
ID znak: parcela [redacted]

katastrska občina [redacted] **parcela** [redacted] (ID [redacted])

Plombe:

Z nepremičnino ni povezana nobena zemljiškoknjižna zadeva, o kateri še ni pravnomočno odločeno.

In addition to real estate related data, the land register discloses details on titles relating to immovable property and facts of legal relevance. All entries in the land register are public. The land register contains principal entries and ancillary entries. The principal entries — incorporations, priority notices and annotations — relate to titles and facts of legal relevance.

Osnovni pravni položaj nepremičnine:

ID osnovnega položaja: [redacted]
vrsta osnovnega položaja: 101 - vknjižena lastninska pravica
delež: 1/1
imetnik:
1. matična številka: [redacted]
   firma / naziv: [redacted]
   naslov: [redacted]
   začetek učinkovanja vpisa imetnika 12.08.2015 [redacted]

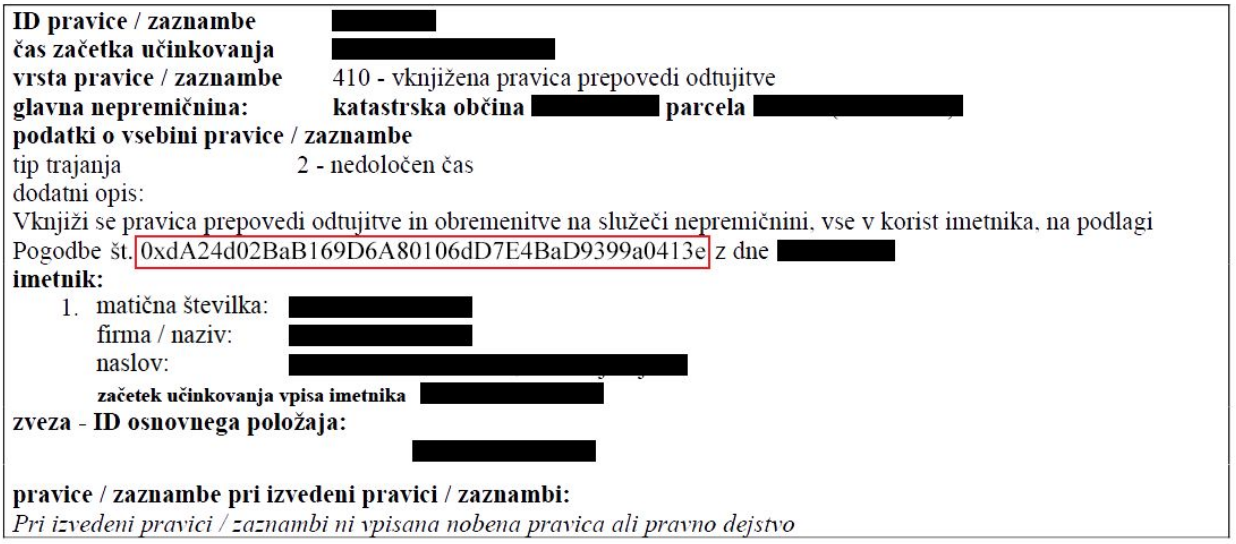
omejitve: **Opozorilo:** v primeru več omejitev z istim časom učinkovanja vpisa se vrstni red ugotovi na podlagi dodatnih opisov pri posamezni izvedeni pravici ali zaznambi.

ID omejitve	čas začetka učinkovanja	vrsta
[redacted]	[redacted]	301 - zaznamba vrstnega reda za pridobitev lastninske pravice
[redacted]	[redacted]	407 - vknjižena služnost stanovanja
[redacted]	[redacted]	410 - vknjižena pravica prepovedi odtujitve

To link a property to the land registry and also provide legal security against fraud, an annotation for *prohibition of alienation or encumbrance* is entered in the land registry. A

[5] Slovenian Land Register. Link: http://www.sodisce.si/javne_knjige/zemljiska_knjiga/

note is then added to this annotation further explaining the annotation entry. In the case of Blocksquare, the PropToken smart contract address is used as legal contract number.


ID pravice / zaznambe [redacted]
čas začetka učinkovanja [redacted]
vrsta pravice / zaznambe 410 - vknjižena pravica prepovedi odtujitve
glavna nepremičnina: **katastrska občina** [redacted] **parcela** [redacted]
podatki o vsebini pravice / zaznambe
tip trajanja 2 - nedoločen čas
dodatni opis:
Vknjiži se pravica prepovedi odtujitve in obremenitve na služeči nepremičnini, vse v korist imetnika, na podlagi
Pogodbe št. 0xdA24d02BaB169D6A80106dD7E4BaD9399a0413e z dne [redacted]
imetnik:
1. matična številka: [redacted]
firma / naziv: [redacted]
naslov: [redacted]
začetek učinkovanja vpisa imetnika [redacted]
zveza - ID osnovnega položaja:
[redacted]
pravice / zaznambe pri izvedeni pravici / zaznambi:
Pri izvedeni pravici / zaznambi ni vpisana nobena pravica ali pravno dejstvo

This off chain legal *hack* allows us to effectively connect a real estate property to its PropToken smart contract counterpart.

On the blockchain side, property related data (i.e. cadastral municipality, parcel number, building number, individual part number, property ID and right ID) and title holder related data (e.g. company's registration ID number, company full name and company address) is inserted in the PropToken smart contract as seen in the example below.

```
// Proof of Title related part

pragma solidity ^0.4.17;
import "github.com/oraclize/ethereum-api/oraclizeAPI.sol";

contract PropToken{

    string public propertyOwnership;
    string public cadastralMunicipality;
    int public parcelNumber;
    int public buildingNumber;
    int public individualPartNumber;
    string public propertyID;
    string public rightID;
    ...

    event IsChanged(address _contract, string _owner, string _changes);
    event OraclizeQuery(string description);

    enum oraclizeState { Ownership, CadastralMunicipality, ParcelNumber, ... }
    struct oraclizeCallback {
        oraclizeState oState;
```

```
    }

    mapping (bytes32 => oraclizeCallback) public oraclizeCallbacks;

    ...

    function checkIFChanged() payable{
        retriveOwnership();
        retriveCadastralMunicipality();
        retriveParcelNumber();

        ...
    }

    ...
}
```

To further induce trust for PropToken holders, the secure ownership verification protocol Proof of Title is triggered on the blockchain. Periodically, for each property, an external third party service is called that retrieves latest information from a land registry and writes it into the blockchain. For land registries providing an API (REST web service), the Proof of Title makes calls through an oracle service (e.g. Oraclize.it) enabling secure and independent information retrieval. The contract checks for information about ownership and other property information and compares new values to the ones stored in the chain. If values differ an event is recorded, notifying the PropToken holders about the change in the land registry.

Oraclize.it is a service offering a trusted bridge between blockchains and traditional non-blockchain data sources on the web. A contract on the blockchain can specify the external data source, which is accessible as JSON or XML via public HTTPS server (or other supported method described in the Oraclize.it documentation). When Oraclize.it API is invoked, the service fetches the information and provides it to the contract, which can store it on the blockchain and use it in computation. Oraclize.it offers cryptographically strong automatically auditable guarantee (TLSNotary proof) that the retrieved content is authentic, i.e. that it was sent via HTTPS protocol with the correct data source's certificate.

Example of API call.

```
// Example (only the code related to communication with Oraclize)

   function __callback(bytes32 id, string result,bytes proof) {
        if (msg.sender != oraclize_cbAddress()) throw;
        oraclizeCallback memory o = oraclizeCallbacks[id];
        if (o.oState == oraclizeState.Ownership) {
            if(propertyOwnership != result){
                propertyOwnership = result;
                IsChanged(this, owner, "Property Ownership has changed")
```

```
            }
        }
        else if(o.oState == oraclizeState.ParcelNumber) {
            ... }
        ...
    }

    function retriveOnwership() {
        if (oraclize_getPrice("URL") > this.balance) {
            OraclizeQuery("Oraclize query was NOT sent, please add some ETH to cover for
the query fee");
        } else {
            OraclizeQuery("Oraclize query was sent, standing by for the answer..");
            // This API doesn't exist at the time of this writing - only an example
            bytes32 queryId = oraclize_query("URL",
"json(https://api.land-registry.gov.si/ownership?cadastralMunicipalityId=1234&buildingId
=54321).owners");
            oraclizeCallbacks[queryId] = oraclizeCallback(oraclizeState.Ownership);
            OraclizeQuery("Oraclize query was sent, standing by for the answer..");
        }
    }

    function retriveCadastralMunicipality() payable returns(bool ok){
        ...
    }

    function retriveParcelNumber() payable returns(bool ok){
        ...
    }
```

Extended validation certificate.

The first part creates a secure and trusted link used to trace title data for a specific property. In Blocksquare's case, the title is held by Blocksquare Foundation serving as a title escrow agent and trusted party.

The second part is proving that the company holding title to a property is also the company that controls all associated PropTokens contracts. The following measures are taken to assure this:

1. Use of an *extended validation server certificate* on the Blocksquare.io website. This class of certificate includes the legal name of the organization which controls the website. The published information can thus be linked to the title holder Blocksquare Foundation, the legal entity serving as a title escrow agent.
2. All PropToken contract addresses and official avenues of information (Slack channels and social media accounts) are always published on the company website.
3. All other best practices for prevention of token spoofing are used (monitoring of blockchain, warnings of discovered threats on social media etc.)

As we wait for land registries to slowly transition to a blockchain system, existing land registry APIs are used for querying real estate property data, title data and facts of legal relevance, giving PropToken holders an automatic and trusted on-chain monitoring system to make sure the Blocksquare Foundation always respects its role as a title escrow agent. In cases when a land registry does not provide an API, PropToken holders need to manually verify title data visiting the online portal of the land registry in question.

Conclusion.

The Proof of Title protocol primary scope is to increase trust amongst users in the Blocksquare network under development. The tokenization of real estate assets is inevitable in the near future and it is critical by organisations researching and developing in this emerging market to follow and integrate high standards of verification and due diligence.

By introducing the Proof of Title verification protocol, Blocksquare openly shows its willingness and constant effort to not only follow but also lead the Blockchain Real Estate industry in a direction towards higher safety standards and fraud prevention methods.