Secure Property Titles with Owner Authority

Nick Szabo

Originally published in 1998

The advent of writing greatly improved the tracking of property rights, and indeed gave rise to our modern systems of property rights and law. However, written records have proven to be quite vulnerable to abuse. A common pattern during eras of political instability or oppression has been the confiscation of land via the forgery or destruction of public records. Reconstruction from informal records, such as residency recorded in phone books, even when possible is costly and fraught with error and potential for fraud[1]. Large amounts of, in some areas most, property in developing countries is not formally titled[2]. Even during eras of political stability in developed countries, there occur many expensive problems with titles.[3] Straightforward transcription of written records into a centralized online repository would make many of these problems even worse – electronic records can be highly vulnerable to loss and forgery, and insiders are the most common source of such attacks. This paper proposes a secure, distributed title database to prevent such attacks against property rights in the future.

Many kinds of Internet resources have a basic characteristic: users must agree on their control across trust boundaries. A big example is names. The article "Names: Decentralized, Secure, Human-Meaningful: Choose Two" dismisses not only the ubiquity and importance of this problem, but also the possibility of solution.[4] Instead petnames are proposed. These are at best mere mnemonics to translate human-readable into cryptographic names; petnames don't do anything to secure naming across trust boundaries. All three attributes – decentralized, secure, and human-meaningful – must be provided if people are to communicate and be communicated about securely over the Internet, and this paper along with the article Advances in Distributed Security shows how to provide all three.

More generally, we show how to implement transferable global rights, enforced entirely by protocol, to names, attributions, bit gold, and similar purely informatic property owned by a particular entity but possessed and relied upon by the public, and how to implement a secure title database for other kinds of property. For a particular example of cross-trust-boundary rights enforced entirely by protocol, see my proposal for name integrity in cross-trust-boundary file systems.

In all cases of property rights there is a defined space, whether a namespace or physical space, and the task is to agree on simple attributes of or rights to control subdivisions of that space. In some cases a name or other symbol corresponds to a person or object owned or controlled by that person. For example, Internet users must agree on which domain name corresponds to which web site operator. In other cases we are simply concerned with control over a subdivision of the space. With real estate we must agree on who owns various rights (to occupy the surface, to mine the minerals under, etc.) to a piece of land. With radio spectrum we must agree on who owns what range of frequencies and in what physical space (or transmitting power as an easily observed approximation of physical space used).

It is the author's hypothesis that all such agreements of control, including control over the semantics of symbols, to be made and respected across trust boundaries are problems of agreeing on and maintaining property rights. Thus the results of this paper are far more general than they might first appear – I believe this paper provides a solution to secure namespaces and similar problems as well as the problem of securely recording agreements on traditional property rights. Highlighting the property rights nature of public directories also highlights the limitations of these mappings – for example that names, addresses, and other

symbols whose semantics are controlled by a person can often be delegated, just as property can be given or rented.

New advances in replicated database technology will give us the ability to securely maintain and transfer ownership for a wide variety of kinds of property, including not only land but chattels, securities, names, and addresses. This technology will give us public records which can "survive a nuclear war", along the lines of the original design goal of the Internet. While thugs can still take physical property by force, the continued existence of correct ownership records will remain a thorn in the side of usurping claimants.

I use political words in this essay as metaphors to describe how our hypothetical property title software, and especially its protocol for distributing the title database across a public network, could work. A group, called a property club, gets together on the Internet[5] and decides to keep track of the ownership of some kind of property. The property is represented by titles: names referring to the property, and the public key corresponding to a private key held by its current owner, signed by the previous owner, along with a chain of previous such titles. Title names may "completely" describe the property, for example allocations in a namspace. (Of course, names always refer to something, the semantics, so such a description is not really complete). Or the title names might simply be labels referring to the property. Various descriptions and rules – maps, deeds, and so on – may be included.

The property club can be thought of as a "microgovernment", an entity that performs globally and independently one narrow function normally associated with government. In particular it is a "constitutional microdemocracy" with low entry and exit costs. After the rules of property transfer have been decided, each vote should stay within this constitution – so that normally the vote will simply implement a distributed operation according to the property rules. The voting is necessary not due to a democratic political ideology but because it is the optimal result in analysis of distributed databases with malicious attackers.[6] If the rules are violated by the winning voters, the correct losers can exit the group and reform a new group, inheriting the old titles. Users of the titles (relying parties) who wish to maintain correct titles can securely verify for themselves which splinter group has correctly followed the rules and switch to the correct group. If the rules are violated by losing voters, they can be excluded from further participation both by correct winners and rule-following relying parties.

This voting-or-reformation method works well where exit costs are low. Thus in practice users should not "put all their eggs in one basket", but different title clubs should be used for different kinds of property. Note that the key security feature of the club is not the voting, but a set of objective, often automated, rules and an unforgeable audit trail that allows both club members and relying parties to check whether each vote followed the rules. So, to go further with the political metaphor, a property club is a "constitutional microdemocracy" with most of the emphasis on the "constitutional". The voting is necessary, but is quite regulated.

To implement a property club, we set up a replicated database so that the club members, hereafter "servers", can securely maintain titles of ownership, and securely transfer them upon the request of current owners. Actually getting end users to respect the property rights agreed upon by this system will be dependent on the specific nature of the property, and is beyond the scope of the current inquiry. The purpose of the replicated database is simply to securely agree on who owns what. The entire database is public.

The ideal title database would have the following properties:

1. Current owner Alice should be able transfer her title to only a single relying counterparty (similar to the "double spending" problem in digital cash)
2. Servers should not be able to forge transfers
3. Servers should not be able to block transfers to or from politically incorrect parties.

We cannot achieve ideals (1) and (3), so we introduce "voting" as follows. A good model of secure replicated databases is the "Byzantine Quorum System" of Malkhi & Reiter[6]. In contrast to most recent work in peer-to-peer software, our design is based on mathematical proofs of security rather than hand-waving. For a short discussion of such threshold-of-servers approaches, see my essay "Coalition Design for Secure Protocols". The database is replicated across a universe of servers U, |U|=n. The "quorum system" is a collection of subsets (quora) of these servers, each pair of which intersect. Each quorum can operate on behalf of the

system; intersection guarantees that operations done on distinct quora preserve consistency. A quorum system tolerant of Byzantine (unconditionally malicious) server failures is a collection of subsets of servers, each pair of which intersect in a set containing sufficiently many correct servers to guarantee the consistency of the replicated data. The authors construct a protocol such that any intersection contains at least 2f+1 servers, thus providing resilience against up to f malicious servers, n > 4f.

Using these results it looks like we can approach our ideal title database as follows:

1. Alice signs the title and Bob's public key, and sends this message to 2f+1 servers, committing her to transfer title to Bob. Bob checks at least 2f+1 servers before relying on Alice's transfer.
2. No collusion of servers can forge Alice's signature (we achieve at least this property ideally!)
3. A conspiracy of >=(1/4)n servers can block a transfer. Alice's only recourse is to use some other channels to broadcast her intention, demonstrating that the registry did not follow her wishes, and hoping the alternative channels are more reliable. Bob only has similar recourse if he signed a document with Alice demonstrating their intentions to transfer title from Alice to Bob. The most basic recourse is a correct subset of servers which exits the property club and establishes a new one, then advertises its correctness (and proves the incorrectness of its rival group) as described above.

Sharing control over property, for example as security for a loan, could be accomplished by sharing the private key corresponding to the current owner's public key. Possession of this private key is required to sign over title; multiparty threshold signatures could also be handled. So it may be a good idea to use one keypair for each combination of title and current owner, rather than keypairs representing the identities of owners. When certain contractual conditions are met, such as the last payment on a loan, this could trigger the generation of a new keypair held solely by the owner, and transfer of title from the shared keypair to the new keypair.

Divisibility and Homesteading

The initial allocations might occur by mapping existing property rights from their current institutional incarnation, or by using traditional methods of staking and negotiating mutual recognition of claims. Some methods less dependent on an existing legal regime for the rights will be discussed in this section.

For some kinds of allocation, such as spatial regions or a hierarchical namespace, we wish to be able to subdivided and re-merge properties. Current owner Alice should be able to transfer various fractional portions of her title to multiple single relying counterparties. One possibility is to have "divide" or "merge" messages whereby the current owner of a property can retire the old property specifications(s) and link them to new property spec(s), the whole message being signed by the owner. Then the new property spec(s) are introduced and considered active, and the old ones considered deactivated. It would be the responsibility subsequent transferees to ensure that the new specifications do not intersect, and are otherwise in good order.

One way to approach the homesteading, or initial allocation, problem, I call the "emergent respect" style: Alice claims the entire unallocated universe. Bob also claims it, the same property spec under a different digital signature. They then may choose to subdivide, sell, give away, etc. property. Each conflicting root grows like a tree into an allocation of all property.

How to resolve trees with conflicting roots? Eventually, the thugs, mechanisms, or informal agreements which enforce property rights converge on a particular tree as the standard, proper allocation. Roots who give away more property to more people, or who actually deploy mechanisms to protect their property, will gain more respect for the tree they started.

In a namespace, conflicts may be resolved by giving names to the conflicting roots, and keeping track of those name-subtree mappings as property.

Usurpers may be able to steal property by setting up their own root and enforcing it, but they can't delete the alternative allocations. The history is always there as evidence for claims.

Those with no firsthand knowledge of conflicting claims may resolve them by consulting authorities, and weighing the opinions of these authorities according to trust metrics, similar to trust metrics sometimes used

for public key certificates.

With secure timestamps, homesteading could be done on a first-come rather than emergent respect basis.

Adverse Possession

For some kinds of property we might want to add the right of adverse possession, or formalized squatting. Here's one general way to implement a kind of adverse possession:

1. Transfers must be securely timestamped.
2. Transfers expire. To maintain ownership, the owner must issue a new transfer to self before expiration.
3. Upon expiration, the property may be homestead on a first-come or emergent respect basis.

This method doesn't attempt to define or utilize a state of "disuse". Instead it equates activity of the property with the ongoing active online presence of an owner who knows about the title and wishes to continue ownership. Cost of maintaining the title might be made high by requiring a periodic registry fee from owners. However, this introduces the problem of who obtains the benefit, by property club rules, of the profits from this fee, and the problem of that the fee lowers the profit of owning the property, even perhaps making it negative. One possibility, where costs of protecting the property are high, is to charge a "Georgian tax" based on some imprecise but objective estimate of the value potential of the property, and allocate the fees to the task of securing the property. To come up with this estimate, or to account for usage of the property itself, would involve mechanisms or observation of characteristics specific to the kind of property, to which subject we now turn.

Correspondence to Ground

Largely unaddressed above is the problem of divergence between actual conditions and directory rights. For example, squatters might legitimately, in the eyes of most property rights enforcers, occupy and improve unused land which a title registry indicates is owned by others. De Soto[2] describes squatters and emergent property rights on the American frontier and today's developing world. When names are property, a name may violate a pre-existing trademark, causing the confusion that both the new namespace and the old trademark namespace were designed to solve.

When divergence becomes too great, a solution to address the unreality of the title registry is needed. One such solution is for the squatters to set up their own rival registry, and then prove the superior correspondence of their registry to actual reality over control and use of the resources. Another solution for squatters is to use the adverse possession mechanism described above – but this works only if the cost of maintaining the title is sufficiently high.

Another solution is to examine the incentives of the titled owner, to see if they correspond to truthfully claiming control over a resource. In most cases there may be incentive to lie, and we can't use this method. In some cases there is incentive to tell the truth and we can, with caveats, rely on it. Any such incentive assumption in the property rules should be explicated, so that relying parties can examine whether the conditions creating the incentive still hold.

Another solution is for property club rules and the registry to originally incorporate rich information about the actual state of property, and modify the actual ownership and transfer on this property based on that state, in a way that leaves few ambiguities so it can be fully audited by club members and third parties. It is most advantageous when this auditing can remain automated, as envisioned above. However the introduction as rule criteria of unrecorded (or unsecurely recorded) transient states common in physical property causes auditing, and thus the titles, to become both less secure and more expensive.

Acknowledgements

My thanks to Gregory Burch, J.D., Eileen O'Connor, J.D., Melora Svoboda, and many others for their helpful comments.

References

1. Kelly McCollum, "Using Phone Books, Scholars Build a Data Base for Resettling Kosovars" ↩
2. Hernando de Soto, *The Mystery of Capital* ↩ ↩
3. Reasons to buy title insurance ↩
4. Bryce "Zooko" Wilcox, Names: Decentralized, Secure, Human-Meaningful: Choose Two ↩
5. Property on the Internet may take all kinds of new forms. For analysis one recently emerged form, the ownership of open source software projects, see Eric Raymond, "Homesteading the Noosphere". ↩
6. Malkhi & Reiter, "Byzantine Quorum Systems", STOC97 ↩ ↩

Please send your comments to nszabo (at) law (dot) gwu (dot) edu