Transacting Real Estate Title using Blockchain Technology

Justin Smith
Elea Labs AG, Switzerland

Dr. Michael Trübestein
Hochschule Luzern, Switzerland

ABSTRACT

A system for recognizing digital title ownership is needed to securely and legally transfer real estate deed at a distance and between untrusted parties. Such a system can be established through the use of a "Web of Trust" and a time-stamping service which relies on the use of the Bitcoin blockchain. The system proposed here assumes simple title transfer and perfect deed, which means the seller controls and is transferring full interest in the property without exception.

INTRODUCTION

Including data in the Bitcoin blockchain can be a controversial topic. Using its blockchain to store application data or for object storage would damage Bitcoin's primary use as programmable money. Therefore arbitrary data of 40 bytes[1] or less may be stored in the Bitcoin blockchain ("blockchain"), and applications should only use this space to maintain references to data stored elsewhere. The time at which a reference is recorded is public and the reference cannot be modified or deleted, which means this can be a useful tool for permanently time-stamping documents.

Documents such as real estate deed can be hashed, and those hashes may be stored in the blockchain. The hash allows anyone to check the integrity of a file, to ensure it has not been tampered with. It's simple to record this hash in the Bitcoin blockchain, but what is missing is the complex social consensus which gives the hashed data the same value as a deed stored in a file cabinet in a land registry office. A procedure for establishing the validity of property deeds prior to inclusion into a blockchain and for legally transferring real estate deed on the same blockchain is proposed here. The Bitcoin blockchain[2] is the protocol of choice due to its immutability and censorship-resistance, properties which are important for securing critical, high value data such as real estate records.

INITIALIZATION

Participants in the transaction must be identified in order to prevent fraud and ensure compliance with local regulations and restrictions regrading deed transfer. By creating a "Web of Trust" (WoT) of Public Notaries can extend notary services to remote users.[3]

NOTARY PUBLIC WEB OF TRUST It is assumed the notary public system is a trustworthy social institution, based on its historic reliability and successful use in diverse regions and cultures. If a network of notaries and land title registries is created using a web of trust implementation[4][5], their current ability to validate the identities and ownership rights of transaction participants can be extended over the internet. The general procedure is as follows:

1. Notary Public Mary in region $R1$ generates PGP public keypair with private key M and public key M'
2. Notary Public Nancy in region $R2$ generates PGP public keypair with private key N and public key N'
3. M verifies N''s identity and control of N'
4. N verifies M''s identity and control of M'
5. M signs N' with ultimate trust
6. N signs M' with ultimate trust

Notary Mary validates the identity of Seller Alice who is in region R1, and Notary Nancy validates the identity of Buyer Bob, who is in region R2, using the same key signing technique. Because of the relationship between Mary and Nancy, both Alice and Bob can trust that each is who they claim to be, without having to meet in person. What criteria are used to establish that someone is actually a notary? Notary publics themselves must decide who is qualified to conduct digital attestation. Based on the research of Lauterbach et. al.[6] on the reputation system used by couchsurfing.com, we assume notaries who are reputable are likely to have their key signed by more notaries.

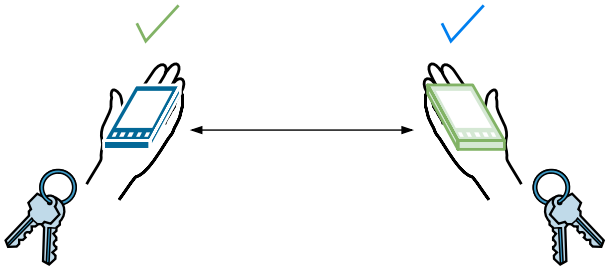

Figure 1: The web of trust procedure may be simplified and secured with the use of mobile devices and/or dedicated hardware.

ESTABLISHING CLEAR TITLE The next step is for a property title insurance provider to conduct a comprehensive title search, where Alice's title and deed to the property are currently maintained, to verify Alice does have the title she claims. First, the property title insurance provider must be identified and added to the Web of Trust.

1. Property title insurance provider Peter in region $R1$ generates PGP public keypair with private key P and public key P'
2. Notary Public Mary in region $R1$ verifies P''s identity and control of P'
3. M signs P' with ultimate trust

Through the notary web of trust, buyer Bob now has confidence that the digital documents signed with P' have been authored by Peter. Seller Alice can now commission Peter to conduct a comprehensive title search to prove to Bob that Alice is offering clear, marketable title. The creation of this comprehensive policy involves establishing a chain of title, tax search, inspection, and name and judgement search. This insurance policy is an important step in every transaction, and should not be omitted.[7] Future policies may be created faster due to the chain of title existing as an immutable digital record, but this transition may take decades. When Peter completes the search and confirms Alice has clear title, Peter creates the insurance policy in digital and traditional formats.

1. Peter creates an electronic document with his findings and insurance policy details. Peter creates a hash of the document, and distributes a copy of the document and hash to Bob and Alice. A matching hash proves the document has not been altered.
2. Peter embeds the hash into the Bitcoin blockchain using the open timestamps standard.[8]
3. Peter distributes the timestamp receipt to both Alice and Bob.

Bob can now have confidence that he will be protected financially in the event the title has been misrepresented.

RESTRICTIONS Because local restrictions and controls are likely to govern real estate transactions, the land registry office, or title office, must be party to the transaction. The same process is followed as with previous transaction participants:

1. Land Registry Ralph in region $R1$ generates PGP public keypair with private key R and public key R'
2. Notary Public Mary in region $R1$ verifies R''s identity and control of R'
3. M signs R' with ultimate trust

TRANSACTION PROCEDURE

1. Alice creates a general warranty deed which includes the hash of the title insurance policy and conveys her ownership interest in the property to Bob.[9]
2. Alice creates a hash of the deed, and distributes a copy of the deed to Bob and Ralph.
3. Alice embeds the hash into the Bitcoin blockchain using the open timestamps standard.[8]
4. Alice creates a 3 of 3 multisignature Bitcoin transaction, requiring signatures from Alice, Bob, and Ralph before it can be spent. The transaction specifies the amount of Bitcoins which Bob will pay Alice for her ownership interest in the property, and embeds the hash of the deed Alice created in an "dummy output" using the OP_RETURN command.
5. Alice sends the transaction to Bob and Ralph.
6. Bob reviews and signs the transaction, and sends it to Ralph.
7. Ralph reviews and signs the transaction, and sends it to Alice.
8. Alice signs the transaction and broadcasts it to the network.

At this point Ralph must check to make sure the transfer has been broadcast, then he can create duplicate paper records if necessary. The transaction is legal and binding; Alice has transferred her full ownership interest in the property to Bob in exchange for lawful consideration, Bitcoin. A distributed file protocol such as IPFS[10] may be used to guarantee access to encrypted copies of the deed and title insurance documents.

SUBSEQUENT TRANSFERS When Bob decides to transfer his ownership interest in the property to a new buyer, Sally, he must follow the same procedure as Alice. But assuming conditions are held constant, title insurance policies can be written with more accuracy and confidence. The title insurance company can check the hashes of the documents kept in the blockchain to the documents themselves to ensure they have not been tampered with. The documents may be kept permanently online using a distributed file system and object storage system, providing additional assurance to the property owner or potential buyer that the records have not been tampered with or lost.

CONCLUSION

The process for simple real estate transactions using a web of trust and blockchain technology proposed here unifies and extends current real estate title transfer procedures. The benefits to using this new process include:

- Timestamping the deed and title insurance with blockchain technology ensures the chain of ownership of real property cannot be lost or modified, even in the event of a war or natural disaster.
- Third parties are not required for facilitating electronic payments in real estate transactions.
- Multisignature transactions involving the buyer, seller and land registry office ensure local rules and regulations may be enforced on every transaction.
- Web of Trust identification practices reduce the potential for fraud.
- Traditional escrow services are not necessary.
- The process can largely be implemented in software.

The system proposed here may be implemented as peer to peer software. Both buyer and seller of the real estate, as well as other transaction participants, would use such peer to peer software in conjunction with a local copy of the Bitcoin blockchain in order to validate transactions for themselves and to prevent being cheated by another party. But real estate title is not the only real property title that can be transacted using this process. An adaptation of such a software could be used to manage ownership changes in virtually any real property title, including boats, cars, and aircraft.

REFERENCES

[1] Rich Apodaca. Op_return and the future of bitcoin. https://bitzuma.com/posts/op-return-and-the-future-of-bitcoin/. Accessed: 2018-04-20.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[3] Jennifer Golbeck, Bijan Parsia, and James Hendler. Trust networks on the semantic web. In *International Workshop on Cooperative Information Agents*, pages 238–249. Springer, 2003.

[4] Patrick Feisthammel. Explanation of the web of trust of pgp. https://www.rubin.ch/pgp/weboftrust.en.html, 2004. Accessed: 2018-05-17.

[5] Mike Ashley, Matthew Copeland, Joergen Grahn, and David A. Wheeler. The gnu privacy handbook. https://www.gnupg.org/gph/en/manual/book1.html, 1999.

[6] Debra Lauterbach, Hung Truong, Tanuj Shah, and Lada Adamic. Surfing a web of trust: Reputation and reciprocity on couchsurfing. com. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, volume 4, pages 346–353. IEEE, 2009.

[7] Anupa Rongala. 5 essential steps of title search process. https://www.invensis.net/blog/customer-service/5-essential-steps-of-title-search-process/, 2015.

[8] Peter Todd. Open time stamps. https://opentimestamps.org/.

[9] Henry Wade Rogers. Delivery and acceptance of deeds. *Cent. LJ*, 13:222, 1881.

[10] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.