Institutions for Equity&Resilience

ANNUAL WORLD BANK CONFERENCE ON LAND AND POVERTY
WASHINGTON DC, MARCH 16-20, 2020

UNLOCKING COMMUNITY LAND TENURE SECURITY: USING DIGITAL KEYS AND BLOCKCHAIN TO SUPPORT COMMUNITY AND INFORMAL RIGHTS

TRENT LARSON, STEPHANIE SAMPSON, JUSTIN HOWARD, AILEY HUGHES
Medici Land Governance, Utah, USA
Trent@MediciLand.com

Paper prepared for presentation at the
"2020 WORLD BANK CONFERENCE ON LAND AND POVERTY"
The World Bank - Washington DC, March 16-20, 2020

Abstract

Lack of clarity around customary and informal land rights can foster land-related conflicts between land rightsholders and the government, between communities, and even between neighbors within communities. There are disconnects between the land rights recognized by a government and those present on the ground. For example, until the Land Rights Act in 2018, the Government of Liberia did not recognize customary land rights as legitimate, resulting in land tenure insecurity and conflicts.

Medici Land Governance and other have applied emerging technologies such as Public Key Infrastructure (PKI), Self-Sovereign Identity (SSI), and blockchain to clarify and protect individual, legal land rights, but application of these technologies to informal and customary rights is still nascent. This paper will explain these technologies in the context of customary and informal land rights and argue for an intervention that uses them for community-based recognition and management of customary and community lands.

Key Words: blockchain, cryptography, customary rights, identity, secure tenure

Lack of clarity around customary and informal land rights can foster land-related conflicts and disputes between land rightsholders and the government, between communities, and even between neighbors within communities. In some cases, there is a powerful disconnect between the land rights recognized as legitimate by a government and those present on the ground. For example, until passage of the Liberia Land Rights Act in 2018, the Government of Liberia did not recognize customary land rights as legitimate, resulting in land tenure insecurity and innumerable conflicts. By clarifying land rights in a way that is transparent and publicly accessible, communities and other informal land rights holders will be better able to protect themselves in the face of conflicts.

Customary Land and Information

There is little recognition of rights in customary land settings, and that recognition is often given hesitantly. National, regional, and city administrators want the confidence that they can implement programs and have consistency in adoption, which is understandable. However, society is complex, and that must be recognized to allow freedom of expression and relationships; plus, the more remote the ruling body (in both locale and communication distance), the less their rules fit life on the ground. We are examining tools whereby communities and even individuals can express their claims in ways that are sustainable and don't endanger the communities.

Despite the drive to formalize all land rights in one system, there are good reasons that informal land rights and agreements exist. First, customary land agreements may have been in place before the formal systems, and there may not be enough incentive to change those agreements. In fact, these agreements may be incompatible with external systems; there may be cultural or historical or conceptual details that may be lost when trying to translate. Second, communities may not get any benefit from interfacing from the external systems. There is always a cost to interacting with other organizations, which may include time, different technologies (and their maintenance), and also an incomplete understanding of the operational norms of the other bodies. Also, the technological barriers are formidable in the developing world.

Finally, communities may be endangered by their interactions with the outside world. One example is with sacred sites such as burial or ceremonial grounds; the members may have specific knowledge internally and they want it to be known externally that the area is protected without revealing the specific location for fear of unwanted visitors or even vandalism. Article 12 of the United Nations Declaration on the Rights of Indigenous Peoples specifically includes “the right to maintain, protect, and have access in privacy to their religious and cultural sites”. Also, with increasing capabilities of correlating data, it’s very possible for outside entities to target and manipulate community members to exploit vulnerabilities in their individual lives or in their position as a member of the group.

Even in the developed world, there is a need for protection of customary land agreements and even data. The Independent Traditional Seminole Nation in Florida is one group who is afraid of further land expropriation, where traditional Seminole spiritual laws do not allow ownership of land; private parties from the outside have created legal entities[1] to help them work together with the external entities. In 2020, Native American groups approached the Library of Congress about culturally sensitive material[2] that should be treated as sacred and not be public.

Globally, there is increasing recognition of indigenous data sovereignty. We show how to share information in ways that respect those principles.

Information sharing between communities and formal systems can have positive benefits for individuals, communities, and governments. Communities benefit by exposing their land tenure claims to the outside world. That exposure can trigger earlier dialogue when governments or investors are considering projects in the area or transfers of rights; this shines light on the dispute early, avoiding conflict later. Internally, more local transparency can provide for better resource management and can help with identification and resolution of local disputes (even if those details are not published to outside entities). Governments benefit in many ways from seeing the community claims. The publicly shared information allows for better implementation of government services, such as taxation and voting rights. The publication of community claims may also help encourage peaceful resolution by proactively recognizing claims that are at risk of being disputed. An active community increases participation in external governmental activities, and an effective community frees up government resources.

Though there are benefits to increasing transparency and clarity on land claims, there are potential challenges to effective implementation. Communities and individuals often avoid the formal system for reasons such as: lacking infrastructure, mobile device availability, bad usability, and a desire to stay

[1] https://indianlaw.org/projects/past_projects/seminole
[2] https://www.usatoday.com/story/news/politics/2020/01/29/native-american-groups-library-of-congress/4599637002/

private (typically due to mistrust of external actors). These technologies alone cannot solve government mistrust or entrenched cultural norms. Community sensitization and social-behavior change must be addressed to allow for profitable communication between communities and the government. Further, though governments rarely avoid engaging with communities since that would be counter to values of fairness and transparency, there may be a risk of outright rejection of legitimacy of a community. This could lead to an unwillingness to engage with certain communities; however, even in those cases, governments benefit from any information provided by the community.

Emerging technologies for land governance such as Public Key Infrastructure (PKI), Self-Sovereign Identity (SSI), and blockchain have been applied to clarify and protect individual, legal land rights, but application of these technologies to informal and customary rights is still nascent. This paper will explain PKI, blockchain, and SSI in the context of customary and informal land rights and argue for an intervention that uses these technologies for the community-based recognition and management of customary and community lands.

Benefits and Barriers of Sharing via Technology

Communities can benefit by using technology to share portions of their information. They can secure better relationships and respect from other governments and communal entities. They can provide proofs of stability for the purposes of contracts & legitimacy. They could get media exposure for more widespread awareness of their issues and their capabilities of interacting with outsiders. They could better demonstrate their losses in case of disaster and demonstrate their legitimacy when seeking contributions or charity.

Earlier, we showed reasons why those in communal environments may not want to share their information; beyond those reasons, there are reasons they may not want to participate in an information network. First, there is a threat of abuse: they may have sensitive information about their region or about their people; this info may be allow external parties take advantage of the community and data science can enable bad actors to manipulate members with increasing reach and rapidity. Second, it may be difficult for members to use the tools: they may not understand why they’re useful or not understand how to make use of them effectively. The efficacy of informational tools relies on the records being up-to-date, so either of those misunderstandings would render the information useless. Third, there is a cost of time and effort to record the information, which may also hinder the timeliness and accuracy of the information. Finally, there are a myriad of maintenance problems: loss or breakage of the devices (including corrosion over time or electrical static or surges), electrical supply failures that may keep them from being used at the time they would be most effective, and simple forgetfulness of how to use the devices and keep them secure.

Technology Aimed at the Barriers

New technologies are being developed to help support individuals and communities with their information needs. For example, blockchain technology (popularized by Bitcoin) is involved in many initiatives that use it specifically for supporting land rights[3].

The success of sharing land claims is dependent on the implementation of emerging tools, such as PKI and SSI, which are based on cryptography, the study of the mathematics of secure data. Besides the community benefits for sharing data with these tools, they enable other features. One is that the data cannot be tampered with later or by others without detection; it is an immutable historical record. Similar to that is the guarantee of authenticity, because others cannot claim ownership for themselves and nobody can modify the record without detection. This avoids corruption by bad actors or mistaken identity. Finally, the record can be authenticated easily without asking for permission. Whoever chooses to share the information can allow the verification of the data with their chosen counterparties.

At a high level: PKI enables individuals to be able to send and receive data in secure ways. They can communicate with certified authorities and partners with the confidence they are sharing with the right entity, and they even establish secure channels where their information is encrypted. Self-Sovereign Identity (SSI) is personal ownership of data. It builds on PKI, but goes further to include even more power to manage identities and verify signatures and secrets. This helps further guard against fraud and enable information sharing in selected ways. Blockchains are publicly managed data storage. Blockchains build on PKI to securely manage the transfer of data "tokens", allowing them to be locked and unlocked only by the intended parties. What makes blockchains remarkable is that they are entirely managed by all participants in a fair way; every member has an incentive to manage the network, but they are secure even with that democratic governance because the balance of incentives of the different players ensures that theft cannot happen without the consent of the token’s owner.

[3] https://cointelegraph.com/news/blockchain-registers-for-recording-ownership-rights-around-the-world

Technologies

This section explains each of the relevant technologies in more detail.

“Cryptographic keys” are large numbers that are hard to guess, and they’re created in a way that they can be used to encrypt and decrypt data. Everyone has some of these keys when they use a computer on the internet. An example in everyday use is a web browser: there is a “secured lock” icon that shows when the user is visiting a secure site, as opposed to an “insecure, unlocked” icon that shows when the site is insecure. Whether a site is secure or insecure is based on a list of “public” keys that the browser knows. That list is a trusted list of sites, which comes installed with everyone’s browser by default; they could add to or remove from that list if they want to mark a site as trusted or untrusted.

These keys allow two significant features:

- Signatures, where someone proves that they are the one who sent the data.
- Encryption, where someone hides data such that only the intended recipient can read it.

Here are more in-depth descriptions of these two features.

When signing data, government, bank, and ecommerce websites with good reputation publish their public key to the world and those public keys are stored in everyone’s browsers. When visitors go to their website, the organization signs the information they send, so the visitor can be sure that it really is the organization expected and not someone pretending to be them. Signatures are purely for validation purposes; they don’t hide any information. They are important for trusting that the data is authentic.

When encrypting data, websites with sensitive information package up their data in a way that nobody in the middle can read it. This uses the same keys as signing, but it goes further to hide the information, ensuring that only the sender and the recipient can read the contents. This is important for credit card numbers and passwords, as well as financial and personal data.

Now we'll describe each of the tools that are built on cryptography for signatures and encryption.

"Public Key Infrastructure" (or "PKI") is a system to manage those cryptographic keys. These are mostly used today by websites that need to preserve their reputation and security. As PKI spreads around the world, users will have keys for their important contacts including people, banks, and government offices. Then when they want to share information, they will use PKI and their keys to sign or encrypt their data.

As an example, Protonmail[4] is an email service where each user gets their own private key. One can send emails the normal way, but one can also choose to use their private key to create signed or encrypted emails to a friend. For this to work, they must first share their public key with the friend; thereafter, their friend can verify the source of the email and even read encrypted emails that are meant just for them. Likewise, if the friend shares their public key with the original person, each can send and receive signed and encrypted messages from one another.

A "blockchain" is a distributed system where the participants can be verified with cryptography, and they usually move tokens between each other. Bitcoin is the first blockchain system to become widely popular. It is a fascinating system because there is no central authority: tokens are created and participants hold them securely in "wallets" that manage cryptographic keys. Only those holders can transfer the tokens; there is no other authority that can take them away without the holder's cooperation.

Another blockchain system called FLO has the additional ability to store messages in the chain; this allows others to verify that the message creator really is who they claim. For example, a land registrar could publish their public key, then create some records on that blockchain; thereafter, everyone could validate that the information was indeed published by that registrar.

"Self-Sovereign Identity" (or "SSI") is the principle that each individual has control of their identity credentials while allowing issuers to provide credentials in a way that preserves confidentiality. Individuals can selectively reveal only slices of the information they authorize.

[4] https://protonmail.com

As an example, universities issue degrees for academic proficiency. The evidence of earning a degree is typically a printed diploma, maybe with the addition of a seal or stamp; to get further confidence, an employer might call the university directly to get someone to attest that the degree was actually earned. It's entirely possible for the university to publish their public key and sign an electronic document which the individual could use for fully electronic validation; however, that document might contain other information that the individual might not want to reveal. With SSI tools, the individual asks the university for a "verified credential" and the individual chooses exactly which information to release to the employer.

"Wifi" is how devices communicate at a close range through the air, eg. in the space of a home, and they have enough encryption capability to sign transactions. There are now wifi devices such as the ESP8266 that only cost about USD$4 each, making it practical to spread a number of them throughout an area, creating a local network. These can be programmed with free, open-source tools that are integrated with toolsets that are commonplace in the computer programming community. They have enough processing power that they can sign and encrypt messages. So, besides enabling wireless communication, these have built-in security features; this makes it possible to selectively share data with only permissioned entities. One benefit for hardware support in these areas is the adoption of basic phones: the power infrastructure already in place could support the use of these small devices.

This could allow for communication within a community, and those utilities may make the tools more attractive and practical for regular use. With electronic message-passing, this also eases the ability to share data with the outside world.

Although these systems are technically ingenious, the power behind these tools comes when many people use them as a group. The more connected and widespread the group, the more utility there is in the network.

How They Can Help Communities

These technologies enable a multitude of improvements in land governance for communities living on customary land.

A community can electronically record decisions internally, then selectively share that information externally. Records can be created with SSI such that they are only allowed to be unlocked and shared to chosen parties. Inside the community, this can enable the group or individuals to assert their own claims and add to their documentation archives. Outside the community, members can choose which records they want to share with formal or public systems; a community might publish their external boundaries or a generic claim of sacred areas without revealing sensitive information.

Further, just like physical records (e.g. for boundary claims), messages can be passed securely and selectively. Basic phones can send direct messages, but SSI-enabled devices can send locked messages and can sign messages to prove authenticity. Inside the community, this can be useful for recording decisions (either from a council or from a broader vote) and recording claims (by internal or external parties). Outside the community, proofs of identity can streamline cooperative work and validate support; a group might publish proofs that there is good internal support for or dispute against external decisions.

Historical documentation can also be secured by an external blockchain. Both inside and outside the community, this can be useful evidence when resolving disputes or researching land claims and usage.

Additionally, credits can be secured with a cryptocurrency blockchain. Both inside and outside the community, this can streamline transactions.

One such example is in Ghana, where residents of one village have discussed with other villages a way to record the areas where their people typically farm. They have discussed maps with color markings that show in red where there are overlaps and disputed areas. One problem with physical, non-networked maps is the difficulty of updating as lines are changed or disputes are resolved. Another problem is the difficulty of sharing the details from one map to another; even if they do not need to be precise, inevitable differences may be undetected or unimportant at first but may become very important later.

Remaining Obstacles

While these technologies break down some of the barriers mentioned earlier, some of the problems remain. Without extra physical protection, the inexpensive hardware is easily corroded. One ideal for hardware reliability is redundancy, but multiple devices compounds the complexity for users. Furthermore, usability is already an issue because the inexpensive hardware has limited interfaces. Touch pads and buttons and LEDs are cheap but limited; displays can help with usability but they are expensive.

When it comes to connectivity, these areas typically don't have standard interfaces to the internet at large. Therefore, achieving wider connectivity will be difficult, even if intermittent connectivity is expected.

With all of these pieces together, we can start pilot projects to address the obstacles and test the validity of all these approaches on the ground.