Scaling up Responsible Land Governance
Annual World Bank Conference on Land and Poverty
Washington DC, March 14-18, 2016

Colored Coins: Bitcoin, Blockchain, and Land Administration

Submitted by:
Aanchal **Anand** (Land Administration Specialist, World Bank)
Matthew **McKibbin** (VP Business Development, Ubitquity LLC)
Frank **Pichel** (Co-Founder, Cadasta Foundation)

Abstract

In May of 2015, news broke that the Government of Honduras was working with Factom and Epigraph to build a land registry system using the blockchain technology that powers the controversial cryptocurrency Bitcoin according to press releases. This sparked considerable interest regarding how blockchain technology might be applied to land administration, with claims that it might revolutionize land information management. Over the course of 2015 however, little additional , detail regarding the venture in Honduras was progressing, culminating in a press release in December 2015 stating that the project was not as far along, nor at the scale, that was originally stated. Regardless, the question of applicability of blockchain for land had entered the public domain, and numerous organizations have begun to look seriously at how they might apply the technology This paper delves into: (a) the blockchain technology; (b) its advantages, disadvantages, and upcoming trends; (c) its relevance to land administration, and (d) a proposed roadmap to test this technology in the context of donor-funded land administration projects.

Blockchain technology is a distributed database maintaining an immutable public ledger of all transactions. This technology is disruptive because it allows for the time stamped accounting of transactions between any party that chooses to use this as a method of recording information. Governments, businesses, and individuals can know for certain the information recorded has not been altered without a record of the change occurring. Decentralized storage of information is done by every node on the network, each maintaining and continuously verifying a complete copy of all transactions. To create a record on the blockchain users submit unique mathematical signatures with privately held computer keys which further helps to minimizes fraud by ensuring authentication of the user. Multi-signature governance accounts allow for increased security by distributing transaction approval over key decision makers involved with the records.

In the context of land administration, blockchain technology has the following applications: (a) title deed registration; (b) time-stamped transactions; c) multi-party transparent governance tools; (d) tamper proof recording system; (e) disaster recovery system; and (f) restitution and compensation in post-conflict zones.

Key Words:

Blockchain, bitcoin, cryptocurrency, land information

Overview - Executive Summary

What is Blockchain?

Cryptocurrencies, or decentralized alternative digital currencies using cryptography to ensure security, have started to enter the mainstream after years of languishing as a fringe technological application. The most well-known of cryptocurrencies, Bitcoin, is now being accepted by traditional retailers from Expedia to Overstock to Microsoft, and can be accessed via over five hundred (500) ATMs worldwide (with most in North America), a number which increased by approximately sixty percent (60%) in 2015 alone. Despite the increased appetite to adopt the cryptocurrency, Bitcoin remains an unstable currency with many questions cast on its long-term viability in the market. In the meantime, much of the excitement is shifting to Bitcoin's underlying technology, the blockchain, which may prove to have a greater impact than the cryptocurrency for which it was built. The potential applications for blockchain are myriad, with claims that the technology can be used to better manage company shares in the financial sector, ensure more complete and secure health records, or even to manage the electoral process.

The interest in blockchain has also spread to the land administration sector, spurred on in part following news in May of 2015 that a Texas based company, Factom, would build a land registry system based on blockchain technology in Honduras, though these claims have recently been shown to be misreported and/or exaggerated. Factom is far from the only company working to apply blockchain to the land sector however, with groups such as Bitland in Ghana, ProSoft Alliance out of Ukraine and Ubitquity from the US all claiming to have integrated aspects of the technology into land system offerings. This paper delves further into how exactly each of these organizations is incorporating blockchain, and what their plans are for the future.

To assess why the blockchain concept might apply to the land sector, it is important to first understand what the blockchain really is. In the simplest terms, the blockchain is a distributed database holding a public ledger of all transactions, each of which is time stamped. What makes the blockchain so innovative is that every node has a complete or partial copy of the blockchain and all historical transactions, eliminating the need for a central database and ensuring that a single user is unable to fraudulently manipulate the data.

What are the Land Administration Challenges?

According to a widely accepted definition first put forth by the United Nations Economic Commission for Europe, land administration includes "the process of determining, recording and disseminating information about rights, value and use of land." Unfortunately, the reality is, despite significant investment by various donor agencies, as well as countless nationally funded land projects, the long term success of implementing land administration systems in emerging economies is woefully poor. Registry and cadastral systems to manage property rights are expensive to develop or configure, they require relatively expensive hardware and software technology which needs to constantly be maintained (and budgeted for), and require technical specialists to administer. In addition to the technical challenges of such systems there are also more fundamental issues to address: poor governance, lack of access to the formal land agencies (particularly for the rural poor), poorly paid staff that are forced to supplement income with rent seeking behavior - which can be traced with a modern land information system, and fear of an easily accessible system that can display the large land holders (who are often the political and economic elite of a country). As a result, these registry and cadastral systems often haven't proven to be sustainable, regardless of whether they are built on open source or proprietary software.

It is no surprise that given these significant land administration challenges, an estimated seventy to eighty (70-80%) percent of the parcels worldwide are not formally registered in any national system. Admittedly this number is at best a ‘guesstimate’, however, most experts working on property rights issues worldwide would generally agree that this is a reasonable estimate. This discrepancy between the number of documented and undocumented parcels only continues to grow, as the number of land professionals remains generally static, while with accelerating population growth and increased urbanization, the number of parcels continues to grow.

How can Blockchain Potentially Address Land Administration Challenges

The concept of a transparent, decentralized public ledger could easily apply to land information management, where the land registry serves as a database of all property rights and historical transactions. The added benefit of using the blockchain technology is that one can get away from a centralized database, which too often could be vulnerable to hacking, misuse by system administrators, or even natural or manmade disasters destroying the data center.

In reviewing potential applications of blockchain technology, some potential uses rise to the forefront, such as: 1) time stamping of transactions akin to virtual notarization; 2) disaster recovery as the system does not rely on a single data center; 3) recording of details in a tamper proof and immutable environment; and 4) utilizing “colored coins” to manage registry details. Each of these potential applications will be expanded upon later in this paper.

Limitations to Blockchain

Detractors of blockchain technology will quickly point out that land administration challenges are largely not a technical problem, but instead an overall governance issue. After all, digital registries and cadastres are a relatively new phenomenon, only becoming the standard in some developed economies in the last twenty years. Prior to the implementation of these digital land information systems, land agencies in developed nations were still largely able to manage rights related data in a relatively expedient and transparent manner.

Simply put, blockchain does not resolve the primary challenge of land administration faced in many emerging economies – how to bring citizens and properties into the formal system. Blockchain will not help to identify who has what right and to where. It will not resolve property rights disputes as properties are brought into the formal system. Most importantly it won’t resolve the tedious and time consuming process of collecting, verifying and bringing data into the system in the first instance.

Furthermore, many of the potential applications of blockchain can be adequately addressed using existing off the shelf technology for land information management combined with improved governance and better standard information technology (IT) practices. Modern land information systems are equipped with security measures which make modification by any unauthorized user very difficult and in any event tracks all changes (even authorized ones) revealing who made them and when. Basic IT management would ensure that data is backed up regularly and stored offsite. Time stamping of transactions could occur when the document is registered formally, or via existing notary services, depending on the specifics of the national law.

Over the course of this paper, the authors will delve further into how various organizations are utilizing blockchain technology for land administration and attempt to draw conclusions regarding best practices and the likely future of blockchain for land administration.

Blockchain: An Overview

Simply put, the blockchain is an economic layer for the internet. It provides a protocol for tokens of value to be transferred on a peer-to-peer (P2P) basis without central actors being necessary. Not only can these tokens be used as a form of currency and a payment system but tokens can represent other forms of value such as stocks, bonds, votes, and even property. The Transmission Control Protocol (TCP)/ Internet Protocol (IP) layer of the internet was designed to transfer packets of information from one computing device on a network to another. The Hypertext Transfer Protocol (HTTP) layer was designed to allow the information to be organized and many layers and applications were built on top spawning the internet as it exists today. The blockchain can be then thought of as the value transfer protocol or the financial internet. The same type of enormous innovation and growth is occurring today to create the new applications and companies one sees at the nascent stages of the internet. The basics of this protocol are described below.

A blockchain is a distributed tamper proof public database which stores its transaction data in containers called “blocks” Each block created is linked to the parent block through digital fingerprints called “hashes.” These hashes are publically timestamped in a header at the top of each block of information. This history of transactions stored on the blocks can be linked back to the initial or “genesis” block. The information stored in blocks is resilient against tampering and corruption even by those who store and process the information. This is made possible by independent nodes that come to a decentralized consensus for all transactions which have occurred. (Antonopoulos, A. (2010))

Keys, Tokens, and Transactions

One of the most important parts of a blockchain system is the keys of ownership and the ability to transact the units of account or digital tokens to other users. This is done using a technology called public key cryptography. Two keys, one public and one private, are used in this system. Keys are stored in a simple database called a “wallet”. The public key creates a publicly shareable address for the user which is normally represented by a unique string of numbers and letters. The private key is the information used to sign the public key and create a unique digital signature. This signature once submitted is used to create a transaction on the network. (Antonopoulos, A. (2010))

Digital tokens are the units of account being kept track of on the blockchain. With different blockchain systems the supply of tokens can be specifically regulated depending on the rules created by its designers. The digital tokens are divisible, fungible within its network, and exchangeable with other networks based upon exchange markets. Companies around the world create these exchanges and charge fees for buying and selling the different digital tokens amongst each other and with governmental currencies. (Antonopoulos, A. (2010))

Bitcoin for example will have a fixed maximum supply of 21 million bitcoins over the course of its entire creation lifetime. Bitcoins are divisible down to the hundred millionth unit. The current price of bitcoin is approximately 385 dollars as of January 23. 2016.

Transactions between users on blockchains are done submitting the unique digital signatures to a network of computers nodes called “miners” maintaining the integrity of the blockchain. These signatures contain the amount and destination for the network to send digital tokens to another address. The transactions and signatures are hashed and compiled into blocks and stored on the blockchain. The transactions are irreversible once stored on the ledger. (Antonopoulos, A. (2010))

Multisignature Transactions

In the transactions discussed prior only one key was required for digital tokens to be transferred to another address. Since transactions are irreversible, this creates a security problem if private keys are stolen or lost by a user. Once stolen the digital tokens cannot be transferred back to the original owner without the private key of the new address.

One solution for the single key signature problem is called a “multisignature wallet.” In this wallet users can choose how many keys signatures are required in order for a valid transaction to be created. For example, 2 of 3 keys could be required in order to create a valid transaction in the network. Many wallet companies now use or require this feature when users create an account for added security. (Antonopoulos, A. (2010))

In traditional corporations or governments, the separation of duties is an important role in governance and accountability. For example, in many companies, the CEO and the CFO have to sign for large expenditures. This governance helps to keep accountability to shareholders and the board within the company. (Morgan, P. (2014, May 25)

Mining and Incentives

For the purposes of this paper the authors will discuss Proof-of-Work (PoW) mining only. See references for other methods of securing blockchains.

Mining is the process of maintaining and securing the blockchain and creating new digital tokens within the ecosystem. This process serves to protect the network against fraudulent transactions and transactions where the same digital tokens are attempted to be sent more than once, also known as a “double-spend.” Miners are given incentives to offer processing power to the network and in exchange new digital tokens are awarded. (Antonopoulos, A. (2010))

Blocks of transactions validated and assembled by miners are recorded on the global blockchain ledger. New blocks containing these transactions vary in time depending on the blockchain network being used. Bitcoin has a new block “mined” approximately every 10 minutes. Once the block is added to the blockchain it is considered to be confirmed on the network. Blocks down on the chain are considered to have additional confirmations equivalent to the number of new blocks before it. The confirmation is required for the new owners of the blocks transactions to access their digital tokens sent to them in the previous block of transactions. (Antonopoulos, A. (2010))

Miners have two separate ways of earning digital tokens. First, on each block miners compete to solve a difficult mathematical problem called a Proof-of-Work (POW). The POW is difficult and energy-intensive to solve but the solution is obtained instantaneously and is easy to verify. The first miner to properly solve the POW is rewarded the new digital tokens after broadcasting and having the solution verified by the rest of the network. Second, miners earn digital tokens by transaction fees associated with each block. The transaction fees are the difference between how much is spent in the transaction and the amount actually sent in the transaction. (Antonopoulos, A. (2010))

Decentralized Consensus

Recordkeeping whether it be on monetary transactions, stock markets, voting records, or land ownership has always been a centralized process. Trust is a key component which individuals, businesses, and government place in those who keep the records for others. There have been countless methods and attempts at making these records and data open, transparent and accountable and those methods continue today through the initiatives of open data and governance organizations. These initiatives still require trust in central authorities to maintain the records.

The most important part of the blockchain invention created by Satoshi Nakamoto was the decentralized mechanism for consensus. This consensus is not dictated by any central authority but is an emergent property of the interactions between thousands of independent computer nodes which follow a set of rules. The blockchain is "the trust machine" in a sense that no one person or entity is required for the records to be recorded and verified. (Antonopoulos, A. (2010)).

This decentralized consensus invention has huge implications for the central organizations which society depends on to keep and verify records. Banks and credit card companies use clearinghouses as middlemen to verify payments and transfers of equities and money between one another. Many companies are now emerging which provide a distributed blockchain which reduces the need for clearinghouses altogether. Banks utilize a shared ledger of the assets, equities and currencies shared between them. (Antonopoulos, A. (2010)).

Furthering the same idea, county clerks or land administration agencies are the centralized record keepers involved in the transfer of land ownership. It is not hard to envision, as these technologies develop, that the public record for land ownership could utilize a decentralized consensus systems. Further in the paper the authors will discuss some of the new companies addressing record keeping of land.

Colored Coins

Colored coins are a a layer developed on top of the bitcoin blockchain. It allows certain transaction outputs to be "colored" or marked by an algorithm representing a particular attribute. The transaction outputs of the digital tokens which are marked with these attributes can represent assets such as stocks, bonds, commodities, or property. The digital tokens, signatures, and keys work in the same way as previously described. Software tools such as a block explorer, wallet, and API have been developed for the colored coins blockchain layer to add functionality to the base software architecture. (Colored Coins. (n.d.)

Hashing for Document Integrity

Information can be embedded into the blockchain transactions allowing for more than just transactional data to be referenced in the future. A hash of a document is created and placed in the data return function of the blockchain called the "OP_RETURN." This feature allows for timestamped proof of existence of documents. If any changes in the information in the document occur the hash will be completely different than the original hash stored in the blockchain. (Antonopoulos, A. (2010))

Limited amounts of data are allowed. One problem which exists is if too many hashes are embedded into transactions. This problem is called "blockchain bloat". Developers within the community discourage large frequency of non-transactional data to be embedded because it has the potential to get close to the maximum memory which can be allowed within each block. Also known as "the block size debate" (Block size limit controversy. (n.d.)). Systems such as Factom aim to address these concerns by adding a data layer to the blockchain and will be discussed further in the paper.

Decentralized File Storage Systems

With the advent of decentralized consensus on a history of transactions, file systems have been proposed and are being built aiming to provide decentralized file storage systems. Using a combination of distributed hash tables, public key cryptography, digital tokens and independently run nodes, file systems allow users to verify file access, integrity, redundancy without a server system or central party providing paid services. Instead of storing documents on a server run by Amazon, Google Drive, or Dropbox, the network provides a data layer of access to documents that exist in many places at once. In this way central points of failure and security risks inherent in the centralized storage of files may be mitigated.

Encryption and Distribution

The different decentralized file systems have security features inherent in each of them. Files are encrypted so as to ensure access to the information is protected from outside attackers. Secondly the files are broken into the pieces and distributed on the network. This allows for files to be stored in many different places at once. Distributed hash tables or Merkle trees are used to keep track of the pieces of each file. These hash tables provide locations of the file pieces and contribute towards ensuring redundancy.

Proof of Integrity

Continual auditing in these systems provides proof of file integrity. The network of nodes within these files systems constantly and upon request verify the hashes of the documents within the system. In this way files cannot be corrupted without notice.

Incentives Via Digital Tokens

In order to incentivize companies and individuals to join the network and offer resources digital tokens are used. These tokens have a dual purpose in this system. First they are used to pay the owners of the nodes and those who contribute storage resources to the network. The user shares their unused storage space from a computer connected to the network and is paid in tokens to his wallet for the native digital token to the network. Secondly the tokens are used to pay for storage space by the clients with the network.

Refer to Addendum A for further detail on the decentralized storage solutions being built today.

Smart Contracts

Smart contracts were originally discussed by Nick Szabo in a small white paper written in 1997. This paper discusses how contractual language and agreements could in theory be encoded and executed by computers on networks without each party in the agreement having to trust the other will make good on their side of the bargain. The first simple example explained is a vending machine. Any person can participate by inserting coins into the machine and the subsequent actions will be taken by the machine to ensure the contract is fulfilled. Szabo, N. (1997)

Eris Industries is one of the leading providers of a smart contracts platform. They describe them as:

"Smart contracts offer a third way [to perform contracts], a new paradigm, wherein legally binding agreements (backed up by real world agreements) can be built to run within a network of computers which no single party can pull the plug on and in which all parties to the agreement participate in the management and supervision of the computers which have automated the agreement." Explainer | Smart Contracts. (n.d.)

Trustless Escrow

Smart contracts allow for services such as escrow to no longer include third parties. Tokens of value either representing currency or assets will automatically be transferred to the other party upon recognition that the conditions have been met within the script of the contract. In the event of a dispute, a third party arbitration service which has been preselected to resolve the dispute will be utilized. These arbitration services can either be governmental or private in nature and many companies and sites have sprung up to fill the arbitration markets providing rating systems for their skill sets.

In many transactions containing property, escrow officers are used as a trusted third party to release the funds and paperwork once conditions are met. Trustless escrow using smart contracts has the potential to greatly reduce the need or eliminate the need for escrow agents.

Blockchain Technologies Appropriate for Land Administration

Colored Coins/Smart Property

Colored Coins are used to represent and track tangible and intangible assets using the blockchain. This feature of the protocol can be applied to land administration by representing the ownership of a piece of land by a single or multiple tokens. The metadata attached to the token can be used to track public registry details such as size, GPS coordinates, year built etc. Details of ownership such as liens, or identity can be encrypted by the land administrator so only those with the correct private key can be shown the information. Any person who is connected to the internet can publicly verify and track the ownership of each token using block explorer software.

The process of representing the land with a colored coin token is called smart property. It can help in land administration because it can provide an easy way to register and transfer a property and help prevent sale fraud. In countries where registration of land is difficult, a low cost certificate of ownership can be issued from a computer. The details tied to the ownership of the token can be stored in the metadata can be found with a web address This facilitates the land administration's duty of having something to refer to as systems become more robust or in the event of a dispute. Private keys may be used to sign documents or transactions to ensure the person is the actual owner. In this way the Colored Coins tokens are a way of preventing sale fraud.

Tokens on blockchain created to represent property are now custom to the same types of computer language and applications discussed in smart contracts. Conditions such as the signing off of a notary, a county clerk or land administrator, and by the owner of property allow for smart contracts around the transfer of property and sale to be executed. Limitless conditions can be met to reduce fraud and for payments to be sent on time. Lenders and title companies can place funds into trustless escrow accounts only to be transferred if payment is received or the proper signatures are presented. (Hearn, M. (n.d.))

Hashing for Document Integrity

The recording of land rights into digital systemsis not yet ubiquitous throughout most of the world. Even in Western countries storing digital files and insuring the data has not been corrupted or is a large problem. One feature the blockchain provides is a timestamped fingerprint of its data called a hash. To fight corruption and track changes as they occur to the documents, hashing can show the chain of custody and help determine whether or not information on the historic documents has been altered.

Title and Deed Registration

Without registration there is no legal proof of one’s land and property ownership. This poses a threat to the owner as his/her rights are not secure and could also have an adverse effect on investment in the country. Without properly registered records, governments and businesses would not be able to identify counterparts (citizens) from whom they need to buy land and/or property in order to invest. Unclear ownership, therefore, has several negative effects on both private citizens and the economy as a whole.

Aside from the challenge to make people more aware of the benefits of registration is the second challenge of getting people comfortable with the registration process itself. In many countries, registration involves several procedures, is time consuming, and often costs a fair amount of money. In 2011, Transparency International noted that land is the second most corrupt sector in the world. This creates a problem of not only lack of awareness but also cumbersome procedures and potential bribes that ultimately discourage owners from registering.

The blockchain technology offers a way in which a hash can be created in the existing registry system to represent a title or deed associated with a particular land or property asset. This transaction is then both time-stamped and tamper-proof, making registration on the blockchain more secure than on any other database that currently exists.

Virtual notary

A notary is a person authorized to perform specific legal functions, generally to guarantee and certify documents, transaction and contracts. The role of a notary varies considerably – in common law countries (such as the US) notary publics require very little training and have little power beyond attesting to a signature, and with 4.8 million notaries in the US, there are no shortage of options. In most civil law countries however – including much of Europe and Latin America, valuable assets can't change hands without a notary's involvement, and notaries are generally trained attorneys. The number of notaries is often capped in civil law countries, resulting in an unnecessary bottleneck for land transactions – both in cost and time. It is worth noting that in the 2008 World Bank Doing Business Report, one of the most effective reforms to improving the efficiency of land transactions was to make the use of notaries optional, particularly as in many cases their role is duplicative with the review conducted by the registrar.

While in civil law countries, notaries have significantly more potential duties, the reality is that one of their primary tasks is certifying documents – a relatively straightforward and simple task that often places an unnecessarily high financial burden on those using a notarial service. Given this relatively easy task combined with technological advances, the process of physically having to meet with someone in order to have them certify a document or any piece of information, could be up for reform.

Utilizing the blockchain is one potential approach for reforming this process, with the blockchain serving as a sort of virtual notary service, authenticating when precisely a transaction occurred and the exact makeup of the contents of a document or contract. In recent years, a number of organizations have popped up offering just this service – for example at Proofofexistence.com – where an individual can simply have a document certified in the blockchain without uploading or transferring the file. Instead, on the individual's computer the file can be "hashed" and linked to the time the document was submitted – thus the proof of existence and contents, as well as the time the document was certified is stored within the block chain. Later if someone re-uploads the document, the system will recognize the file only if it is the exact same document. Even the slightest change in the document, the "hash" would be completely different.

Multi-party Transactions (Including Marital Property)

An important land administration application that can be derived from the multiparty signature feature or multiparty wallets is security women's property rights when it comes to marital property. Anecdotal evidence from several countries suggests that even when women legally have equal rights to land and property, these rights are not socially followed or respected. Husbands sometimes sell marital property without their wives' consent so multisignature wallets could go a long way in protecting women's rights to marital property. Other applications of multiparty transactions could involve property transactions involving several owners as in the case of acquiring a small business loans with the joint property used as a collateral.

Disaster Preparedness

Due to its ability to store tamper-proof records on the public ledger, another potential application of blockchain is the development of blockchain-based disaster recovery center. The idea is similar to what has already been discussed—storing registry records as hashes on the bitcoin blockchain. The main drawback of this idea is that there may simply not be enough memory to transfer these records to the blockchain. This could improve as the technology develops and the blockchain becomes more nimble to deal with big data. It would also depend on government willingness to store all records on the blockchain, and more generally in “the cloud” and not on national soil - something many governments have been reluctant to do.. If this could be achieved, blockchain could change the landscape in terms of disaster preparedness as well as helping with post-conflict restitution and compensation as tamper-proof, time-stamped ownership records will be available through the blockchain ledger.

Decentralized Storage and File Management

Decentralized storage systems combine hashing of documents and redundancy of storing encrypted records in more than one place. These features solve some of the problems typically found when storing records on a centralized server. Land administration records if stored or backed up on a decentralized storage system are protected against fraud, and allow for disaster recovery.

Summary

Potential Application	Pros	Cons	Likelihood (or example if underway)
Colored Coins			
Hashing for Document Integrity			
Title or Deed Registration			
Virtual Notary			
Multi Party Transactions			
Disaster Preparedness			
Decentralized File Management			

Blockchain for Land Today

Non-Profit and for profit companies are aggressively working to develop land specific software solutions on top of the blockchain. Open source protocols, such as those integral for the cryptocurrency and blockchain applications, are usually developed under the guidance of non-profit foundations for governance and fund management purposes. Many of these foundations then spawn for profit companies to take on enterprise customers. Land administration is traditionally a responsibility of governments, many companies interested in the land sector are actively engaging the government land agencies and land professionals for guidance on how to better create products which have a better chance of adoption. Ultimately government buy in is crucial for these systems to be implemented, particularly in emerging economies.

Non Profit

Factom Foundation

Factom Foundation is a non profit organization which supports the open source development of the Factom Protocol; a scalable data layer for the blockchain. This is a similar model to the Mozilla Foundation which promotes the web as a public resource, while wholly owned subsidiary Mozilla Corporation,manages the open source development of many of Mozilla products. More can be found on Factom.org .

Omni Layer Foundation

The Omni Foundation is a non profit organization (originally Mastercoin) which was created in the Fall of 2013 to manage the funds and the software development of the Omni layer. The Omni layer is a meta layer which builds on top of the blockchain software architecture to enable new types of features such as smart property, The platform is engaged with enabling decentralized applications such as Factom and Maidsafe built on top of bitcoin and other blockchain systems. An apt analogy for describing the Omni Layer is to compare it to the protocols built on top of internet such as HTTP to TCP/IP.

From Their CFO Patrick Dugan; "The Omni Layer Foundation (short: Omni Foundation) seeks to combine market making, interest free loans to Bitcoin dealers in developing countries, and technology development. We are looking at simple Real Estate Investment Trusts in developed jurisdictions and working with BitLand in Ghana. The open source technology we have published is a protocol for an asset layer over the Bitcoin blockchain, which includes as soon to be activated decentralized exchange."

Bitland Ghana

Bitland is a non-profit organization that is working to keep the land registration process accessible, transparent, and free from government corruption. They plan to streamline and automate the entire land registration process so it provides a better system of record that digitizes land titles and keeps the databases on a distributed system with multiple fail-safes. In order to properly ensure communication between the working group within Bitland and the external liaisons, a very direct communication system must be developed (Security Program Best Practices, 2013) having a working group communication hierarchy to ensure that the project's goals are reached, and the responsibilities within the organization are clearly defined and followed.

As the company works to update paper data storage of land into digital format, it also consolidates new land registry requests against the old registries. In many cases, the official documents are outdated, and the locals have their own systems for keeping track of titles. In order to get a single registry that represents a consistent ledger of land title holdings, all of these problems must be solved, and in the process the integrity of the central registry must be kept.

With the consent of the Ghana Land Commission, the organization is currently in the process raising funds to start a road show visiting all ten regions of Ghana to educate communities about Bitland land title documentations and take field exercises to record a thousand properties in each region inthe Bitlanddatabase, digitally timestamped on the blockchain with an encryptedsystem that uses a combination of decentralized data storage and traditional server warehouses for back-ups, and includes GPS coordinates for each property. e The road show is designed and organized by Bitland to reach the necessary funding to implement and expand our operations by establishing a purpose-built service center in every region that will further assist our capacity to develop the skills, educate, counsel and provide land title solutions to the people of Ghana that will help the country grow by incorporation.

So far Bitland has been funded privately by the founder and CEO, Narigamba Mwinsuubo, as well as Factom. Currently the organization is smaller than 50 employees including ambassadors, regional administrators, campus coordinators and community representatives of which everyone is working pro bono. Bitland is based in Kumasi, Ghana, and is looking to expand operations into other countries in the African continent within the next few years.

Honduras

In mid-2015, news emerged that Factom and Epigraph were in talks with the Government of Honduras to pilot a land registry based on blockchain technology. For months there was no further comment on this initiative and whether the right funding had been secured. In an interview to CoinDesk in December 2015, Factom CEO Peter Kirby noted they had received a letter of intent from the Honduran government to record land titles for Honduras's fourth largest city La Ceiba on the blockchain. As of now, it appears that the initiative has been halted. In the same interview Kirby spoke about "difficulties of working with global governments on land title projects" and "addressed past questions about the validity of the initiative."

For Profit

Factom Inc.

Factom Inc is the for-profit subsidiary of the Factom Foundation, dedicated to serving enterprise customers who want to develop on the Factom protocol. Factom raised $3.4M in 2015 and are valued at $11M, and according to press releases, has partnered with the government of Honduras to provide a land registry application.

Ubitquity LLC

Ubitquity LLC is focused on the development of a blockchain based system for the tracking of ownership of real estate titles in US markets. They are currently in the late stages of development of a minimal viable product (MVP). Their platform creates a colored coin token to represent ownership of a property which is transferred over the blockchain. The parallel recording system along with digital signatures and hashing of deeds and title documents is aimed at reducing conveyance fraud. Partial ownership, of tokens for liens and multisignature governance features can be implemented for added security. More can be found at (http://www.ubitquity.io)

ProSoft Alliance

Prosoft Alliance is a company focused on the provision of efficient land administration through the use of innovative technology, combined with advisory services by land information professionals with global experience. ProSoft Alliance has developed an open source, workflow and rule based land administration software product, InnoLA.

Recognizing the potential interest by partners and clients in blockchain technology to further ensure tenure security, ProSoft has worked to integrate blockchain via the Factom data layer into the InnoLA software. Working with Factom, ProSoft developed a proof of concept workflow which enhances the functional task of verifying and committing data (such as the recording of a deed). As part of the deed recording or title registration process, the responsible authority conducts a final "verify and commit" task, which when executed, opens a new window to "sign and seal the dataset," inclusive of the core attributes deemed critical, which are then hashed and sent to Factom's distributed network of servers. Upon successful submission to Factom, the entire transaction becomes read only and can no longer be edited.

Subsequent access to the committed specific transaction within the InnoLA system by either the registry office or the general public via web access, includes functionality to "validate" the transaction, which will compare the unique hash of the current dataset stored in InnoLA with the transaction hash permanently stored in Factom. Depending on the result, a positive or negative message will be displayed, the Factom Explorer page is opened and automatically navigates to the specific entry related to the transaction.

As a next step, Prosoft will extend their integration with blockchain to allow for a full review of transactions, in essence demonstrating the "chain of title" or the historical transactions for a specific property.

Summary Table

Project	Location	Status	Funding	Scope	results	Next Steps
ProSoft Alliance – InnoLA Software	Global	Proof of Concept Blockchain Integration	-	-	-	
Factom	Austin, TX	Beta Factom Protocol	$11M	Global		
Ubitquity LLC	Global	Developing Proof of Concept	Prefunding	US Land & Title		Pilot to Launch in Q2 2016
BitLand	Ghana					

Conclusion

Even though bitcoin continues to be a highly volatile currency, its underlying technology—the blockchain—may prove to be a game changer. The blockchain's key feature of being a time-stamped public ledger has earned it the name "trust machine." What this essentially means is that blockchain technology can help increase transparency and conduct transactions more securely.

For this reason, the blockchain has several applications for land administration. Some of the applications discussed in the paper include smart property (colored coins), title deed registration, virtual notary, multiparty transactions, and disaster preparedness. The paper also notes that some of the applications might be more relevant for mature economies as compared to emerging economies. Furthermore, the paper notes that many of the potential benefits of utilizing the blockchain assume that a base layer of land information (titles, deeds, survey plans) exist and that the data is accurate - an assumption that is not valid in most emerging economies.

The paper also gives an overview of the various players involved in developing land administration applications of the blockchain. Given that blockchain is a relatively new technology, there is a fair amount of excitement in the field as various applications and business models are tried. Three major constraints that have been identified. First, while the proof of concept has been established it exists on a small stage.

The major challenge will be to see whether or not blockchain based land transactions are in fact scaleable and if yes, does a viable business model exist to support such a venture. Second, part of the scale problem lies in getting government buy-in. Even Factom, which has been leading this space, has acknowledged that it is not easy to get governments excited about new technology which has not been tested widely. Third, funding constraints exist around the development of blockchain for land administration. As of now there seem to be two major options. One is for developers and companies to turn to crowdfunding. The second is for donors to take a greater interest in this technology and see if it could help tackle several developing world challenges linked to property rights and corruption. It appears that the blockchain could be the silver bullet that tackles both these issues. But much remains to be seen.

References

A scalable data layer for the blockchain. (n.d.). Retrieved January 19, 2016, from http://factom.org/

Antonopoulos, A. (2010). *Mastering Bitcoin*. O'reilly Media.

Benet, J. (n.d.). IPFS - Content Addressed, Versioned, P2P File System. Retrieved January 19, 2016, from https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf

Benet, J. (2014, July 15). Filecoin: A Cryptocurrency Operated File Storage Network. Retrieved January 19, 2016, from http://filecoin.io/filecoin.pdf

Block size limit controversy. (n.d.). Retrieved January 19, 2016, from https://en.bitcoin.it/wiki/Block_size_limit_controversy

Colored Coins. (n.d.). Retrieved January 19, 2016, from https://en.bitcoin.it/wiki/Colored_Coins

Explainer | Smart Contracts. (n.d.). Retrieved January 19, 2016, from https://docs.erisindustries.com/explainers/smart_contracts/

Hearn, M. (n.d.). Smart Property. Retrieved January 19, 2016, from https://en.bitcoin.it/wiki/Smart_Property

Irvine, D. (n.d.). Maidsafe Whitepaper. Retrieved January 19, 2016, from https://github.com/maidsafe/Whitepapers/blob/master/Project-Safe.md

Mizrah, A. (n.d.). A blockchain-based property ownership recording system. Retrieved January 19, 2016, from http://chromaway.com/papers/A-blockchain-based-property-registry.pdf

Morgan, P. (2014, May 25). Multi-Signature Accounts for Corporate Governance. Retrieved January 19, 2016, from https://empoweredlaw.wordpress.com/2014/05/25/multi-signature-accounts-for-corporate-governance/

Mougayar, W. (2014, December 14). The Blockchain is the New Database, Get Ready to Rewrite Everything. Retrieved January 19, 2016, from http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/

Omniwallet™ - The Next Generation Wallet. (n.d.). Retrieved January 19, 2016, from https://www.omniwallet.org/about

Snow, P. (2014, November 17). Factom Business Processes Secured by Immutable Audit Trails on the Blockchain. Retrieved January 19, 2016, from https://github.com/FactomProject/FactomDocs/raw/master/Factom_Whitepaper.pdf

Szabo, N. (1997). Nick Szabo -- The Idea of Smart Contracts. Retrieved January 19, 2016, from http://szabo.best.vwh.net/idea.html

Szabo, N. (2002). A Formal Language for Analyzing Contracts. Retrieved January 19, 2016, from http://szabo.best.vwh.net/contractlanguage.html

Wilkinson, S. (2014, December 15). Storj A Peer-to-Peer Cloud Storage Network. Retrieved January 19, 2016, from http://storj.io/storj.pdf

Wilkinson, S. (2014, December 23). MetaDisk A Blockchain-Based Decentralized File Storage Application. Retrieved January 19, 2016, from http://metadisk.org/metadisk.pdf

https://medium.com/@Stampery/can-blockchain-technology-send-notaries-on-vacation-for-good-4b99df14de7d#.pnftllgxh

ANNEX A

Refer to Annex A for more details on the decentralized storage solutions being built today.

Storj

A peer-to-peer cloud storage network implementing end-to-end encryption would allow users to transfer and share data without reliance on a third party data provider. The removal of central controls would eliminate most traditional data failures and outages, as well as significantly increasing security, privacy, and data control. A peer-to-peer network and basic encryption serve as a solution for most problems, but we must offer proper incentivisation for users to properly participate in this network. We propose a solution to these additional problems by using a challenge algorithm. In this way we can periodically cryptographically check the integrity and availability of a file, and offer direct rewards to those maintaining the file. In absence of a peer-to-peer network the described methods may be used to allow users to control, migrate, validate their data on 3rd party data providers without the provider having direct access to the data. (Wilkinson, S. (2014, December 15).

IPFS

The InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. In some ways, IPFS is similar to the Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high throughput content-addressed block storage model, with contentaddressed hyper links. This forms a generalized Merkle DAG, a data structure upon which one can build versioned file systems, blockchains, and even a Permanent Web. IPFS combines a distributed hashtable, an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and nodes do not need to trust each other. (Benet, J. (n.d.))

FileCoin

Filecoin is a distributed electronic currency similar to Bitcoin. Unlike Bitcoin's computation-only proof-of-work, Filecoin's proof-of-work function includes a proof-of-retrievability component, which requires nodes to prove they store a particular file. The Filecoin network forms an entirely distributed file storage system, whose nodes are incentivized to store as much of the entire network's data as they can. The currency is awarded for storing files, and is transferred in transactions, as in Bitcoin. Files are added to the network by spending currency. This produces strong monetary incentives for individuals to join and work for the network. In the course of ordinary operation of the Filecoin network, nodes contribute useful work in the form of storage and distribution of valuable data. (Benet, J. (2014, July 15))

Maidsafe Network

The SAFE network [ref Network] utilizes a mathematically complete, peer-to-peer Public Key Infrastructure (PKI) authorization on an autonomous network [ref Autonomous], secured key-value storage and reliable Kademlia based routing [ref Routing]. The network is designed to be decentralized and has the ability to get rid of Domain Name System (DNS). The PKI solution deployed within the SAFE network validates a user's identity with mathematical certainty. (Irvine, D. (n.d.))