Colored Coins: Bitcoin, Blockchain, and Land Administration



Written By: Aanchal Anand, Matthew McKibbin, and Frank Pichel

Paper prepared for presentation at the "2017 WORLD BANK CONFERENCE ON LAND AND POVERTY" The World Bank – Washington DC, March 20-24, 2017

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.

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?

How can Blockchain Potentially Address Land Administration Challenges

Limitations to Blockchain

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

Mining and Incentives

Decentralized Consensus

Colored Coins

Hashing for Document Integrity

Decentralized File Storage Systems

Encryption and Distribution

Proof of Integrity

Incentives Via Digital Tokens

Smart Contracts

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

Multi-party Transactions (Including Marital Property)

Disaster Preparedness

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.

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

Bitland Ghana

Honduras

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

ProSoft Alliance

Summary Table

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

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

Addendum A

Refer to Addendum A for futher detail on the decentrlaized 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.))