COMPUTER SYSTEMS, INC.

A Presentation for

Blockchain – What does it mean for the Indiana Recorders Association

April 24, 2019

Sources: Blockchain Technology

The following slides are based on sources and comments taken from the following publications:

- Dr. Gideon Greenspan – **MultiChain Developer Q & A**. (https://www.multichain.com/blog/author/gdg/)
- John Mirkovic, Cook County Records of Deeds - **Blockchain Cook County – Distributed Ledgers for Land Records Cook County Recorder of Deeds Blockchain Pilot Program – Final Report** (https://illinoisblockchain.tech/blockchain-cook-county-final-report-1f56ab3bf89)
- International Blockchain Real Estate Association (IBREA) - **Blockchain for Title and Conveyance (https://www.ibrea.network/)**
- State of Vermont - **Blockchain Technology: Opportunities and Risks** (https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf)
- **Real Estate on the Blockchain: Is Tokenized Property a Reality in 2019? (https://blockexplorer.com/news/real-estate-on-the-blockchain-is-tokenized-property-a-reality-in-2019/)**

Blockchain & Real Estate

Blockchain first achieved its notoriety with Bitcoin. Bitcoin was a new means to tokenize currency that bypassed traditional means for the exchange of money (e.g. banks, brokerage, SEC etc.). Tokens are a means to reduce risk in handling high value financial instruments by replacing them with surrogate equivalents.

Most of the real estate activity using Blockchain has been to tokenize Real Estate transactions with the goal to disintermediate trusted intermediaries. Blockchain as a real estate registry has been mostly attractive internationally because of weak or non-existence land registries. By far the largest interest of blockchain for real estate has been to tokenized real estate transactions like Bitcoin or Ethereum. The tokenization of real estate opens up the market to investors that might not be able to afford a full property or even the high minimums of traditional real estate investment trusts (REITs), provide the ability to crowdfund for real estate development projects or to buy and sell real estate especially in countries who do not have sophisticated and trusted intermediary like the SEC. For more information, visit International Blockchain Real Estate Association (IBREA) - Blockchain for Title and Conveyance (https://www.ibrea.network/).

In the USA, the State of Vermont and Cook County IL (Chicago) have investigated the use of Blockchain for their land registry. Many start-up companies are testing Blockchain for use in the tokenization of Real Estate as a financial instrument. See https://blockexplorer.com/news/real-estate-on-the-blockchain-is-tokenized-property-a-reality-in-2019/ and one start up company called velox.RE who is trying to replace paper property deeds with electronic deeds.

These findings have been referenced in this presentation.

Why use a Blockchain System?

"A distributed ledger is a system that allows parties who don't fully trust each other to come to consensus about the existence, nature and evolution of a set of shared facts without having to rely on a fully trusted centralized third party." (https://www.multichain.com/blog/2016/12/spot-half-baked-blockchain/)

The Core Value of a Blockchain is to eliminate the need for trusted third-party intermediaries in some transactions (e.g. Banks, Brokerages, Government agencies, Recorders etc.).
This is why most of the Blockchain applications today are financial transactions (e.g. Bitcoin, Ethereum etc.) that seek privacy NOT transparency to the rest of the world.

If implemented for records management and preservation, the goal may be by some to get rid of (disintermediate) the Trusted Recorder and their current local land records management systems that is already fully trusted.

Which Blockchain?

Blockchains or Distributed Ledger Technology (DLT) removes the need for a central database operator (Trusted Intermediary) and replaces it with numerous databases spread across a Peer-to-Peer network. Peer-to-Peer was first used in 1979 for the World Wide Web. Remember Napster? It too was a Peer-to-Peer system. The inherent problems of a Peer-to-Peer network necessitated and spawned the need for a trusted centralized database system.

Which Blockchain?

1. Public Blockchain (associated with Cryptocurrencies like Bitcoin and dozens more)
2. Permissioned or Enterprise Blockchains (associated with cryptocurrency Ethereum and more)

Both implement shared database using Peer-to-Peer networking, public-private key cryptography, transaction rules and consensus mechanisms that can survive malicious actors. **They are different in terms of confidentiality, scalability and governance.**

Conditions for a Blockchain

Conditions for a Blockchain

There are a bunch of conditions that need to be fulfilled if you are going to adopt a Blockchain.

And if the conditions are NOT met, you should go back to the drawing board. Maybe you can define the project better. Or maybe you can save everyone a load of time and money, because you don't need a blockchain at all.

The Conditions:

1. A Database
2. Multiple Writers
3. Absence of Trust
4. Disintermediation
5. Transaction Interaction

Conditions for a Blockchain

1. Shared Database – Blockchain is for those who don't trust a trusted centralized database and they substitute it with numerous copies of a shared distributed database that is visible to every node (e.g. computer) on the blockchain network.
2. Multiple Writers – Blockchain is a shared distributed database with multiple writers (e.g. banks, mortgage companies, private citizens, IRS, Courts etc.).
3. Absence of Trust – Blockchain is technology for a shared distributed database across numerous computers with multiple non-trusting writers. Each writer doesn't trust the Recorder or other unknown writers to read or write to its database.
4. Disintermediation – Blockchain removes the need for a trusted intermediary (e.g. Recorder) by enabling software (vs a human) that allows multiple non-trusting writers to modify the database directly.
5. Transaction Interaction – Blockchains truly shine where there is some interaction between transactions created by multiple non-trusting writers. One transaction is dependent on another transaction.

Conditions for the Blockchain

If implementing land records management on the Blockchain **does NOT fulfill every single one of these conditions**, you should NOT be using a blockchain.

In the absence of a yes for any of the first five conditions, you should consider one of: (a) regular file storage, (b) a centralized database, (c) database replication (RAID, DRaaS), or (d) multiple databases to which users can subscribe.

And if you do fulfill the first five, there's still work to do.
You need to be able to:

6. Set the Rules - What Rules (e.g. Smart Contracts)?
7. Pick your Validators - Who approves a data entry?
8. Back your Assets - Who is responsible for the assets in the system?

Conditions for a Blockchain

What Rules?

If you are going to replace the human Recorder as a writer (data entry) and allow multiple non-trusting writers to enter data directly to the distributed databases, the system must contain embedded software (e.g. Smart Contracts) with the data input rules. What rules?

1. How to restrict what transactions can and cannot be performed?
2. What about historical records, how do these records and transaction history get entered?
3. How do you reject a recording?
4. What Index data to collect (e.g. grantor/grantee, parcel ID, legal description, consideration etc.)? Look at eRecording issues regarding trust for those non-trusting writers collecting the data.
5. What are the document types and document subtypes?
6. How to redact confidential information on a Document that is hashed?
7. What documents are confidential and should not be visible on a public blockchain?
8. What data can be accepted (e.g. misspellings, punctuation variances, proper abbreviations, what data requirements etc.),
9. How to verify the document (what document type, what document subtype, was it notarized, was it signed, is it even for the correct County/Blockchain etc.).
10. Etc. etc. etc.

You are replacing a trusted human writer with Smart Contracts. Look at eRecording and would a Smart Contract solve all of these problems and questions with eRecording?

Then you other Rules:

1. What kind of hashing/cryptography (e.g. MD5, SHA-1, SHA-2, PBKDF2, ARGON2 etc.) and
2. What kind of encryption (e.g. key) of the data and documents (e.g. the password protection for nodes/Validators and Smart Contracts). **If you lose the key or the key is hacked, then what??**

Smart Contracts vs Humans

A Smart Contract is a fancy name for software code which runs on a blockchain. In the database world it is called stored procedures.

Who Does the Data Entry?

Since there will be NO fully trusted human third party or trusted intermediary (e.g. County Recorder) to validate the data entry, you need software to replace the human. In the Blockchain world this trusted software is called a Smart Contract.

"*A smart contract is a password protected piece of code which is stored independently on each node on the blockchain, triggered by blockchain transactions, and which reads and writes data in that blockchain's database*."

Are Smart Contracts Smart?

Who validates the data entry?

Because the blockchain is a "*consensus-based system*", this only works if every Validator/node/computer on the Blockchain reaches an identical state after processing every Smart Contract transaction and block. You can have NO differences. The moment that two honest nodes disagree about the Chain's state, the entire system becomes worthless.

Because Smart Contracts are executed independently by every Validator/node and the source of data is outside the Blockchain, there is no guarantee that every node will receive the same answer. Perhaps the source will change its response in between the time of consensus, or perhaps it will become temporarily unavailable? Either way consensus is broken and the entire Blockchain dies.

Workaround?

One or more trusted parties (e.g. Recorder?) retrieves the data and creates a transaction which embeds that data in the blockchain.

Are Smart Contracts Smart?

Because the source of data is outside the Blockchain and every node is independently executing the Smart Contract in the chain, who is responsible for creating the information? If the answer is one node, what happens if that particular node malfunctions, deliberately or not?

If the answer is every node, can you trust every node with the private key (e.g. encrypted passwords) to perform that responsibility?

What if the node loses that private key/password? If the private key/password is stored on a computer can it be hacked? Do you really want hundreds of nodes with an private key/password?

Workaround?

A trusted party could watch the transaction and creates the transaction in the blockchain. The blockchain plays a passive role.

Need Workarounds?

Looking at these two workarounds, we can make some observations.

1. They both require a trusted entity (e.g. County Recorder) to manage the interactions between the Blockchain and the outside group of actors. While technically possible, it does undermine the goal of a decentralized Blockchain system.

2. The mechanisms used by the workarounds are straight forward examples of a human using a trusted centralized system for reading and writing to a database.

The “trusted” Smart Contract which provides the external information is simply writing information to the chain just like in a human in a trusted centralized database.

Conditions for a Blockchain

Who are your Validators & why do you trust it (not a human)?

The Blockchain is to be the authoritative final transaction log on whose contents all nodes (e.g. computers) on the Peer-to-Peer network must provably agree.

Why do you need a transaction log? This allows newly added nodes to calculate the database's contents from scratch, it also addresses the possibility that some nodes might miss some transactions (system down), if two transactions are in conflict only one can win and for precise ordering of transactions.

You need to be confident about the software (e.g. can it be hacked?) and your Validators.

Who are you Validators?
How do you pay the miners (e.g. nodes on the blockchain)?
How many Validators (one or many)?
What kind of distributed consensus algorithm (e.g. PoW, PBFT etc).
Why do you trust the Validator?
How do you resolve conflict?

Conditions for a Blockchain

Two ways Validators can unduly influence a database's content.

1. Transaction Censorship. If enough Validators collude maliciously (e.g. hacked by China, Russia, North Korea, Iran etc.), they can prevent a particular transaction from being confirmed in the Blockchain.
2. Biased Conflict Resolution. If two transactions conflict, the Validator who creates the next block decides which transaction is confirmed on the blockchain, causing the other to be rejected.

Because of this you need to have a clear idea of who are your Validators and why do you trust software vs a human ? Do you have one or more Validator nodes controlled by a trusted single entity (e.g. are we back to needing a Recorder?), or a core group organizations (e.g. SOS, IRA, Private Equity company, Wall Street Company etc.) that maintain the chain or every node on the network is a Validator?

Conditions for a Blockchain

Who is Backing Your Assets?

"*Blockchains are mainly of interest to those who track the movement and exchange of financial assets. I can think of two reasons for this: (a) the finance sector is responding to the (in retrospect, minuscule) threat of cryptocurrencies like bitcoin, and (b) an asset ledger is the most simple and natural example of a shared database with interdependent transactions created by multiple non-trusting entities.*"

If you do want to use a blockchain as an asset ledger (e.g. land records), you need to answer two additional crucial questions: **What is the nature of the assets being moved around and Who stands behind the assets represented on the blockchain?**

If the database says that I own this land, who will allow me to claim that land *in the real world*? Who do I sue if I can't convert what's written in the blockchain into the traditional physical assets?

Pointless Blockchain?

Are people searching for a problem to a solution?

How many Counties in Indiana have had a court case where a person or entity was accused and convicted of fraudulently altering a recorded document or index data stored in a County Recorder's land records management system?

Avoid the Pointless Blockchain

BLOCKCHAIN FINDINGS AND WARNINGS

"*At present, the cost and challenges associated with the use of blockchain technology for Vermont's public recordkeeping outweigh the identifiable benefits.*"
(State of Vermont)

"*Compared to Relational Databases that have been deployed on millions of servers running trillions of queries, blockchain technology is still in its diapers.*"
(Dr. Gideon Greenspan)

"*The use of blockchain with a Proof of Work consensus algorithm that requires expending massive amounts of electricity to confirm each transaction is not ideal for real estate recordkeeping. Distributed ledgers may be a better option.*"
(John Mirkovic, Cook County Recorder of Deeds)

Trust the Recorder vs Software?

Trustworthiness is primarily based on Reliability, Accuracy and Authenticity of the record (Color emphasis below are mine).

"Blockchain technology does not address the reliability or accuracy of a digital record."

"…if bad data is used as an input, as long as the correct protocols are utilized, it will be accepted by the network and added to the blockchain."

"If a document containing false information is hashed as part of the properly formatted transaction, the network will validate it. Furthermore, the network is unable to distinguish between a transaction by an actual user or a malicious transaction by someone with unauthorized access to the user's private key."
(State of Vermont https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf)

Pointless Blockchain

"***If your requirements are fulfilled by today's relational databases you'd be insane to use a blockchain***"
(Richard Gendal Brown, CTO of R3
https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/).