doxpop™

blockchain

New Yorker Cartoon by Peter Steiner from 1993… And also the problem we're trying to solve:
Trust in an electronic environment.

This presentation will dig a little deeper into the issues raised by your last presenter about the authenticity of digital copies.

Blockchain in 30 seconds:

- A electronic record that can never be changed. (Like a recorded document.)
- With signatures that can never be denied. (Like a notarized document.)
- Distributed storage. (Robust, consensus-driven.)
- Becomes stronger with every new entry, because each “block” contains the “hash” of every previous block. (Think of amber accumulating around a fly.)
- ***Does not require a trusted third party*** (Look out, Recorders!)

doxpop™

Blockchain is ***not*** bitcoin or any of the other cryptocurrencies.

Blockchain is simple technology that is most useful as a method of verifying the integrity of an original record. That makes cryptocurrency possible, *but they aren't the same thing.*

- Concepts:
  - Pointer
  - Cryptographic (one-way) Hash
  - Distributed ledger
  - Consensus (voting)

A “pointer” is just what it sounds like:

- A pointer tells us where to find a piece of data.
- The instrument number (or book/page) in your indexing systems is a pointer: It tells us where to find the document data we care about.

A “hash” is like a fingerprint...

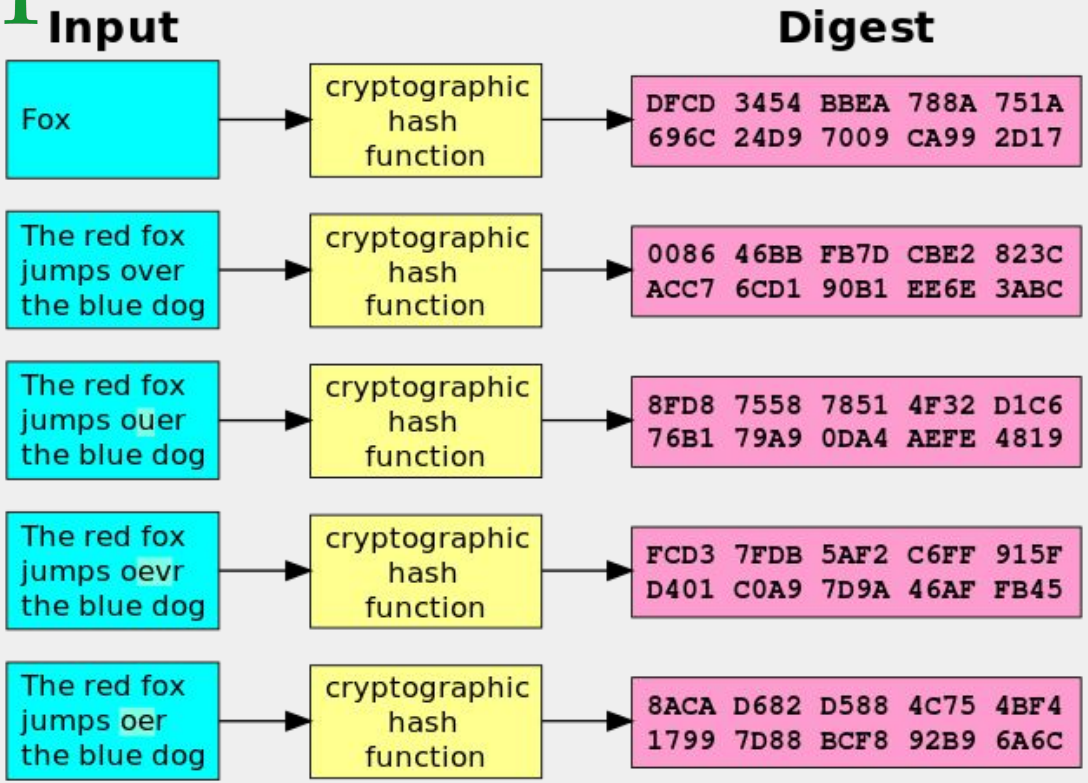
- Suppose a=1, b=2, c=3, etc...
- The hash of “cat” is 24 (3+1+20). Change it to “rat”, and the hash changes to 39.
- Now apply this to every letter in a document. If you change any letter in the document, the fingerprint changes.

(Please don’t use this hash for real work! It is simple and flawed… Only useful to understand the concept.)

doxpop™

The SHA-1 Hash function in action:

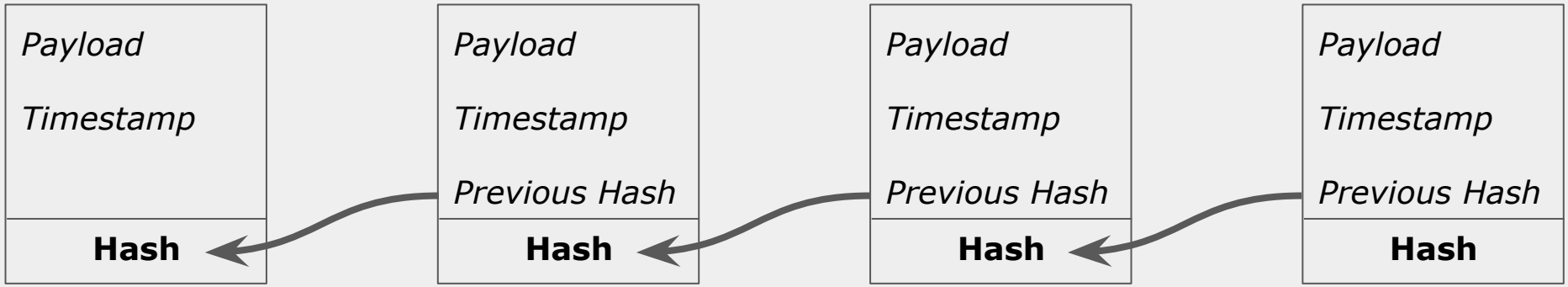
blockchain



Now we know enough to create a simple block chain:

Each Block contains:

- A pointer to the previous block.
- The hash of the previous block.
- A “payload” (That’s your data, like a document.)
- The hash of this (current) block.



Because the hashes are “chained” any block can be used to verify all previous blocks because if the payload is changed in one block, the hash in every following block would have to change.

Now we add robustness: Distributed Ledger

- Anyone who exclusively controls the entire chain can still alter it. That's a trust problem.
- *So everyone who cares keeps their own copy.*
- Every time a block is added, everyone verifies the hash using their own copy and checks to see if they agree.

And finally, integrity: Consensus

- Every time a block is added, everyone verifies the hash using their own copy and checks to see if they agree.
- If they don't, everyone votes on the correct hash.
- Whoever loses has to delete their chain and replace it with a chain that matches the majority.

It's like Lori's *internal controls* on steroids.

Who maintains these copies of the ledgers?

- In **public blockchains** like Bitcoin and Etherium, nodes are paid to do the work of maintaining the system, and authorized to vote by proving that they have skin in the game (Proof of Work or Proof of Stake.)
- In **private blockchains** each node maintains copies and is authorized to vote by mutual agreement.

Digital storage is great because it is so easy to make backup copies.

The challenge is how to verify that you have true copies.

Blockchain solves that problem.

Cyber Currency:

- Cryptocurrencies like bitcoin just store and move value, same as a dollar bill, but through the Internet.
    - Can’t be spent twice.
    - Can’t be taken back.
    - No trust needed.
    - It’s exciting, but not as exciting as smart contracts...

Smart Contracts:

- Smart contracts can be used to execute transactions of many types, and may involve any number of participants. Once put on the blockchain, they can't be changed or removed. (Kind of like recording a document…)
- We need to think about the evolving role of the Recorder and local government in this environment and plan for it.

A simple smart contract:

If you put $0.75 into the coin slot, and press the button corresponding to the drink you want, you will receive that drink.

- The contract is written on the outside of the machine.
- The contract is executed without human intervention every time you fulfill your part of the contract.

For instance:

- Bob is willing to pay Alice $100,000 for her house.
  - The offer is good for 30 days.
  - The offer is contingent on the home inspector providing a clean report.
    - If a problem is found, the inspector can provide an amount to be deducted for repair. This adjusts the sale price downward.
  - The offer is contingent on Alice purchasing title insurance.
  - The document is Recorded when the auditor makes the tax transfer.
  - When the document is recorded, the courts will enforce the contract.

These conditions can be built into the contract so that it automatically executes if each of the five participants “signs” with her or his or her electronic certificate.

doxpop™

blockchain

Challenges for local government:

- Who owns the parcel?
- Who gets the tax bill?
- Was a split or combine involved?
- Which parcel is being transferred?
- What was the price?
- What about enforcement if there is a dispute?

The Recorder still has an important role, *but not just as trusted third party.*

Most important:

- The implementation of blockchain in land records should be a move toward an open and shared system.
- It is critical that any enabling legislation *set standards for open competition instead of choosing winners* that will end up controlling access to transactions and records that should be in the public domain.

doxpop™

blockchain

Steps that the Recorder's Association may want to take:

- Start by recording the hash of current paper facsimile documents on a blockchain. This adds a "fingerprint" for every document and extremely robust integrity checking. (No legislation required.)
- Provide an interface to receive the documents directly from smart contracts. (Might already be covered by UETA)
- Allow smart contracts to replace the paper documents. (Legislation required to facilitate.)

How step one might work:

- A document is recorded in any county.
- A hash is immediately calculated for the document image. The image and hash are shared with all 92 counties.
- Each county adds a block to their copy of the ledger. The “payload” for the block is the county, the instrument number and the hash for the document image. (It could also include the index.)
- A quick vote is taken to agree on the hash of the block for that document. Now the document can *never* be changed.

doxpop™

blockchain

How step one might work: (continued)

- We don’t need to duplicate the document images in every county, just the hash. (But we could)
- The hash can be used to verify any copy of the document, so it can (and should) be shared publicly and freely.
- Since the hash is one-way, it can be used to verify an image, but the image still needs to be purchased.

Why bother? (Let me tell you a story…)

doxpop™

blockchain

Find this presentation online at:

http://bit.do/Doxpop_IRA2019