**Course Name:** Blockchain: How Does it Work? Do CPAs Need It?

**Speaker:** Kelce S. Wilson, PEDDal

**Course Description:**
The reasons for why blockchains can provide a trust mechanism, even among parties that otherwise have no basis to trust each other, will be explained, along with other widely-discussed (but usually unexplained) aspects of blockchains: cryptocurrency, document protection, and mining. Both benefits and problems with blockchains will be described, along with an explanation of recently-reported threats to blockchains from advances in quantum computing. The applicability of blockchains to protecting financial documents from forgery will be described in sufficient detail that attendees will be able to immediately start planning how to incorporate blockchain use into areas of their practice where it makes sense to do so.

**Learning Objectives:**
Participants will:
1. Understand how a blockchain can be leveraged to render documents (including financial records) tamper-evident, so that forgery can be readily detected.
2. Understand the differences between using a blockchain for protecting documents and for trading in a cryptocurrency.
3. Identify which aspects of blockchain systems are relevant to document protection and which are relevant to cryptocurrencies.
4. Understand why blockchain-protected data can generally be trusted.
5. Understand some of the limits of blockchains.

**Category:** Basic/Technical

**Prerequisites:** None
Blockchain: How Does it Work? Do CPAs Need It?

Kelce S Wilson, JD, MBA, PhD
kwilson <at> softwareipattorney <dot> com

29 April 2019
What We will be Covering

- What is a blockchain?
- How are blockchains related to Bitcoin?
  - And cryptocurrencies, and distributed ledgers
- Can you use a blockchain to protect important documents from forgery attempts?
  - Quick answer: Likely, yes
- What parts of a blockchain are relevant to protection of documents?
  - How to protect documents such as:
    - Estate planning documents (wills, codicils, trust documents)
    - Contracts
    - Financial records (bank statements, transaction ledgers)
    - Even website pages that hackers might try to forge
- Example of using a blockchain for document protection:
  - Alice’s Will - Detection of a forgery attempt
Where Are We?

• What is a blockchain?
• A description of how it works
• “Trust in the absence of a trusted entity”
• How are blockchains related to Bitcoin?
• How to use a cryptocurrency
• Using a blockchain for document protection
• What parts of a blockchain do you really need?
• What does it look in operation?
• Example of using a blockchain to detect a forgery

Want to know more? Send a message to QUESTIONS <at> PEDDaL <dot> com
What is a Blockchain?

• In general, there are three ways to describe something:

  1. How great it is ⇒ What it can do?
     • Call this “the commercial”

  2. How to use it ⇒ What can you do with it?
     • Call this “the user’s manual”

  3. How it functions ⇒ What actually makes it work?
     • Call this “the blueprint”

How many presentations have you sat through on blockchains, hoping to learn how it worked, but all you heard was: “Blockchain is great and it is going to change everything!”

Nice, … but … exactly HOW does a blockchain function?

No worries. You’ll be finding out soon. And it isn’t really all that difficult to understand.
What is a Blockchain?

• First, the obligatory “How great it is” pitch:
  • A blockchain permits you to trust information that is given to you:
    • By someone you do not know
    • When you have no other solid basis to trust that person or the information itself, and
    • No one, whom you do trust, can endorse that person or the information
      • How many opportunities have you passed up because you were unable to verify the authenticity of some information that you were given?
      • How many opportunities have you lost because someone did not trust you?
      • Imagine the freedom you would have if trust in critical information was easier!
  • A blockchain provides “trust in the absence of a trusted entity”
    • This is a key concept
      • Very powerful
What is a Blockchain?

- And, now a quick “How to use it” explanation for cryptocurrency:
  1. Person A receives a cryptocurrency unit X (which is just a string of digital data)
  2. Person B receives a cryptocurrency unit Y
  3. B then spends Y – but beware: unlike paper money, digital data is easy to duplicate
  4. Some time passes
  5. A and B try to purchase something from person C, who has no basis to trust either A or B
  6. So, C checks the cryptocurrency ledgers in the proper blockchain and finds that:
     1) Since the particular ledger entry that shows A receiving X, of all the subsequent ledgers (in the different blocks of the blockchain), **none shows A spending X**
     2) Since the particular ledger entry that shows B receiving Y, of all the subsequent ledgers (in the different blocks of the blockchain), **at least one shows B had already spent Y**
  7. Therefore, C detects that
     1) A is still the true owner of X
     2) B is attempting to double-spend Y
  8. Which, of cryptocurrency units X and Y, will C accept?
What is a Blockchain?

• And, now a quick “How to use it” explanation for legally-significant documents:

  1. Person A creates a document and “puts”* it into a blockchain at that time
  2. Several years pass
  3. Later, … person B forges a version with information favorable to B and detrimental to A
  4. Person C needs to settle a dispute, and has no basis to trust either A or B over the other
  5. So, C “checks”** the proper blockchain and finds that:
     1) A’s version is proven to be several years old and is also possibly digitally signed
     2) B’s version has no history in the blockchain, or perhaps only a much shorter history
  6. Whose version is C more likely to trust?

• Additional steps may indicate that a document was endorsed by someone, when it was first put into a blockchain
  • In the example at the end, Alice’s lawyer endorses the document with a digital signature

* “puts” requires some amount of explanation; it will be provided later
** “checks” requires some amount of explanation; it will also be provided later
What is a Blockchain?

• Now, … “How it functions” … starting with …

• A couple of definitions:
  • “Tamper-proof” means that something cannot be altered
  • “Tamper-evident” means that, if something is altered, others are likely to notice
  • Consider a medicine bottle at the store with a plastic wrap around the cap
    • tamper-proof or tamper-evident?

• And a primer on “hash functions”:
  • NO, not something you smoked during college
  • A mathematical function that treats computer files like just a set of numbers
    • *.DOC files, *.JPG files, *.MP3 files, *.PDF files, … anything
    • The program you use with these documents is irrelevant - only the binary bits matter
    • The result is a “digital fingerprint” of the file, and usually expressed in Hexadecimal
      • 0 through F, rather than 0-9, with A=10, B=11, C=12, D=13, E=14, and F=15
      • So x10 (hexadecimal 10) is actually the number 16 in the familiar decimal system
    • Some common hash functions are named SHA-1, SHA-256, SHA-512, and MD5
What is a Blockchain?

- A blockchain is a set of information blocks that are related using a mathematical algorithm
  - You can keep your own copy if you want; you can download one from multiple sources
  - A hash function “chains” the blocks together in a unique sequence
  - If a block is altered by forgery, and the true one is available anywhere, all honest observers will use the true one and reject the forgery
    - The altered (forged) block will simply not fit within the sequence; and
    - If the true block is not available, there will be a noticeable gap in the sequence
  - You can trust a sequence to be complete and intact if the math solves properly
    - There are no missing blocks – the information is complete – and no extras (forgeries)
    - **You can believe in the chain, even if you do not trust anyone else involved with it**
    - Hash functions are standardized; you can use any copy that you trust (even write your own!) to independently test the blocks and ensure that the chain is assembled properly
  - Blockchains can leverage this simple certainty to generate trust in larger systems, much like a brick can be used as a single unit to construct larger buildings of various shapes
What is a Blockchain?

- The SHA-1 hash of “abc” is “A9993E364706816ABA3E25717850C26C9CD0D89D”
- The SHA-1 hash of “abd” is “CB4CC28DF0FDBE0ECF9D9662E294B118092A5735”

- Good hash functions have some properties worth mentioning here (there are others):
  1. If a file does not change, it always produces the same hash value with the same function
  2. If a file does change, even by the smallest amount, the hash value will change drastically
     Note how different the hash values are for “abc” versus “abd”
  3. Any two different files (or data sets) should have different hash values
     When two different files produce the same hash value, this is called a collision
  4. It is too difficult for anyone, who knows a particular hash value, to create a new file that (when hashed) will produce that particular hash value
     This is called a preimage attack
     A second preimage attack is the intentional creation of a collision with two different files
     A successful second preimage attack on SHA-256 would likely undermine Bitcoin.
  5. They are one-way, so knowing a hash value does not give any information about the file
     Even publicizing the hash value for a document still preserves confidentiality
What is a Blockchain?

Consider these five blocks of data:

```
7A14E377C203E79B1430
9B1803E87B14D9C54A22
TTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTTT

A9993E364706816ABA3E
25717850C26C9CD0D89D
IIIIIIIIIIIIIIIIIIIIIIII
IIIIIIIIIIIIIIIIIIIIIIII

49EDC148DE3C6F2433A4
A4207EAFD0FD351993EB
GGGGGGGGGGGGGGGGGGGG
GGGGGGGGGGGGGGGGGGGG

23D9F2F82FE8D14D7A62
D3CDDE7F7405AB4A65EF
BBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBB

A9993E364706816ABA3E
25717850C26C9CD0D89D
IIIIIIIIIIIIIIIIIIIIIIII
IIIIIIIIIIIIIIIIIIIIIIII

23D9F2F82FE8D14D7A62
D3CDDE7F7405AB4A65EF
BBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBB

49EDC148DE3C6F2433A4
A4207EAFD0FD351993EB
GGGGGGGGGGGGGGGGGGGG
GGGGGGGGGGGGGGGGGGGG

What do we know about them?
What is a Blockchain? Detail to read on your own, later

Consider these five blocks of data:

What do we know about them?

Not much really, except that two of them are similar and differ by only a single character:

One has the SHA-1 value for “abc” followed by 40 “I’s”

Another has the same SHA-1 value followed by 39 “I’s” and then one “X”
What is a Blockchain? Detail to read on your own, later

- We will use the following process:
  1. Hash each block with SHA-1
  2. Look for the hash value of each block in each of the other blocks
  3. We know that, even if someone knows a hash value, they cannot use it to figure out a new block. Therefore, if the hash value of one block (“block A”) is found inside another block (“block B”), then we know that **A must have already existed when B was created**

We can put the blocks in the sequence in which they were created, using hash values

**All honest observers independently create the same sequence**, recognizing when:
  1. Any block is missing; and
  2. A block that is provided along with a group does not belong in the group

- If a block is altered, but the true one is available, all honest observers will use the true one
- If a block is altered and the true one is not available:
  - The altered block will not fit within the chain; and
  - There will be a gap where the altered block should have fit
What is a Blockchain? Detail to read on your own, later

The SHA-1 of:

- A9993E364706816ABA3E
  - 25717850C26C9CD0D89D
  - I I I I I I I I I I I I I I I I I I I I I I I I I I I I

is

- 7A14E377C203E79B1430
  - 9B1803E87B14D9C54A22

and is found within

- 7A14E377C203E79B1430
  - 9B1803E87B14D9C54A22
  - TTTTTTTTTTTTTTTTTTTTTTTTT

---

- 7A14E377C203E79B1430
  - 9B1803E87B14D9C54A22
  - TTTTTTTTTTTTTTTTTTTTTTTTT

is

- 23D9F2F82FE8D14D7A62
  - D3CDDE7F7405AB4A65EF

and is found within

- 23D9F2F82FE8D14D7A62
  - D3CDDE7F7405AB4A65EF
  - BBBBBBBBBBBBBBBBBBBBB

---

- 23D9F2F82FE8D14D7A62
  - D3CDDE7F7405AB4A65EF

is

- 49EDC148DE3C6F2433A4
  - A4207EAFD0FD351993EB

and is found within

- 49EDC148DE3C6F2433A4
  - A4207EAFD0FD351993EB
  - GGGGGGGGGGGGGGGGGGGGG

---

- A9993E364706816ABA3E
  - 25717850C26C9CD0D89D
  - I I I I I I I I I I I I I I I I I I I I I I I I I I I I

is

- 2CC44532A406A9C09163
  - 6F4A1A00D48533EC9584

and is found within

- 2CC44532A406A9C09163
  - 6F4A1A00D48533EC9584
  - NOT FOUND ANYWHERE!
What is a Blockchain?

• This is what we know, now:

1. The block with the 40 “I’s” was created before the block with 40 “T’s”
2. The block with the 40 “T’s” was created before the block with 40 “B’s”
3. The block with the 40 “B’s” was created before the block with 40 “G’s”
4. Therefore, the blocks were necessarily created in this order:
   1. “I’s”
   2. “T’s”
   3. “B’s”
   4. “G’s”
5. This particular chain tells us nothing about when the block with 39 “I’s” and one “X” was created (Other than it was after someone had hashed “abc” with the SHA-1)

• You can believe these statements to be true, even if you do not trust me

• Blockchains can leverage this simple certainty to generate trust in larger systems
  • Much like a brick can be used as a single unit to make larger buildings of various shapes
Where Are We?

• What is a blockchain?
• How are blockchains related to Bitcoin?
  • Are they the same thing?
  • Some people use the terms interchangeably
• How mining works
• The lurking threat to all blockchains
• How to use a cryptocurrency
• Using a blockchain for document protection
• What parts of a blockchain do you really need?
• What does it look in operation?
• Example of using a blockchain to detect a forgery
How are Blockchains Related to Bitcoin?

• Bitcoin is a cryptocurrency with several important aspects:
  1. Tokens – this is what people can collect and spend
  2. Ledger – this is the list of transactions, indicating the current owner of a token
     The ledgers are publicly readable so others can search for double-spending attempts
     That is, **if the ledgers can be trusted to be complete and free of alteration**.  
        *But we know how to do this now! Use a blockchain to reveal forgery attempts!*
  3. Blockchain – this is the trust mechanism that proves the ledgers have not been altered
     Remember the blocks with 40 “I’s” versus 39 “I’s” and one “X”? (in the detail section)
     It was easy to figure out that one fit the chain in a particular position; the other did not fit
     **Forged ledgers won’t fit within the blockchain**; they will produce the wrong hash value
  4. Consensus – a distributed community votes on adding blocks to the chain
  5. Mining – members of the community solve a math problem using a nonce
     This is how new token are created, too complex to explain here.  *See me at the break.*
  6. Independent, duplicated storage – every node keeps a full copy of everything
  7. Anonymity – Not really perfect anymore; tools can track token recipients and spending
How are Blockchains Related to Bitcoin?

• Something important to note:
  • Definitions of the word “blockchain” can vary greatly
  • Some people equate blockchain with cryptocurrency
    • According to people with that type of view, something missing even one of:
      • Tokens
      • Consensus
      • Mining
      • Independent, duplicated storage
    … is simply “not a blockchain”
  • Don’t worry about the different definitions
    • Even the original Bitcoin document did not use the term “blockchain”
      • The phrase “blocks are chained” described only the sequencing of blocks via a hash
    • Just be aware of them, and clarify when you hear someone using the word blockchain
      • There is a chance that the person might not even know what definition they are using
How Mining Works in Bitcoin

- First, an explanation of the non-uniqueness of a hash value:
  - A hash function maps a file (no matter how long), into a fixed number of bits
  - The SHA-256 maps files into a set of only 256 bits (32 bytes)
  - The issues are difficult to portray visually with 256 bits, so we will use an example of mapping to two bits (a byte is 4 bits in many computers):

    | File  | Hash |
    |-------|------|
    | AAAA  | 00   |
    | BBBB  | 01   |
    | CCCC  | 10   |
    | DDDD  | 11   |
    | EEEE  | ??   |

    We ran out of numbers. One of them must be reused.

- Whenever you hash enough different files (more than $2^{256}$ for the SHA-256), at least one of the hash values (message digests) **must be reused**
  - When two files have the same hash value, this is called a **collision**
  - In general, for an arbitrary set of N bits, there must be at least N/256 possible collisions.
  - For a 5Mb file, the theoretical minimum number of collisions for a single hash value (if collisions are evenly spread in probability among the values) is about 160,000
**How Mining Works in Bitcoin**

- The security of a hash function is not that no one can find a collision, but instead that it is just very difficult
  - The SHA-256 has over $100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000$ possible different values
  - So we still have a way to go before running out of different values

- Some definitions repeated here, to put them in perspective:
  - A **collision** is when two different files have the same hash value
  - A **preimage attack** is when someone creates a file match a specific hash value
  - A **second preimage attack** is when someone creates a second file to match the hash value of a first file, and the first and second files have different content
    - A **second preimage attack** is a forced collision with files having different content
    - A hash value cannot reveal a forgery that uses a successful second preimage attack
    - This is why the feasibility of successful second preimage attacks against SHA-256 can undermine confidence in Bitcoin
  - Bitcoin mining can be viewed as a **partial preimage attack**, in which the goal is to find a file that matches part of a specific hash value: the first 18 bits are zero
How Mining Works in Bitcoin

- Bitcoin uses a block header containing:
  - a version number;
  - the hash of the previous block (reversed)
  - the Merkle root of the block contents (reversed)
  - a timestamp
  - a count of the bits
  - and a **nonce**

- The **nonce** is a set of bits that can be any number

- The operation is:
  - a starting value is assigned to the nonce
  - the block is hashed with the current nonce
  - does the hash value start with 18 zeros?
    - if not, repeat: change the nonce (increment?) and try again
    - if yes, then submit the block to the community for the vote

- The nonce is not 256 bits (it’s 32)
  - This means that a collision is not guaranteed
  - To force a collision, maybe change the timestamp and/or add some transactions

- If you find a “magic nonce” first (there is more than one!), you might win the token
  - Network propagation and latency issues add complexity to the consensus operation
**The Lurking Threat to All Blockchains**

- Consider a file with a first hash value
  - Break it up into three portions:
    1. A portion to alter (e.g., erase a transaction in which you had spent Bitcoin value)
    2. A portion to keep intact (e.g., perhaps most of the rest of the file, to prevent detection)
    3. A portion that can be used to force a successful second preimage attack
  - Initially, before you make any changes, the file has a first hash value
  - You alter portion #1 to suit your preferences
  - The altered file now has a second, different hash value
  - You then manipulate portion #3, perhaps by adding or altering bits in a manner that is designed to minimize the likelihood of anyone noticing
    - The file now has the first hash value again
    - Anyone who relies upon only hashing the entirety of the file (without doing more) will not detect your forgery
    - Note that Bitcoin has some complicating factors, such as the Merkel root of the content. So a good forgery will require more than just one successful second preimage attack.
  - **Threat from quantum computers is possible feasibility of a second preimage attack**
Where Are We?

- What is a blockchain?
- How are blockchains related to Bitcoin?
- How to use a cryptocurrency
  - What do you need to do?
  - Can you just go in a little bit, or is it a huge commitment?
- Using a blockchain for document protection
- What parts of a blockchain do you really need?
- What does it look in operation?
- Example of using a blockchain to detect a forgery
What is needed to get into a cryptocurrency?

• There are two levels of involvement in a cryptocurrency:
  1. Spender, holder, investor – just a purchaser with no involvement in growing the chain
  2. Miner, node owner – a community member who helps grow the chain (via consensus)

• A spender merely needs to obtain a digital wallet
  • You will need an app on your phone or computer
    • You will need to create a special digital identification for yourself
    • Consider using a hardware wallet, for the additional security
  • Convert between regular currency and cryptocurrency using an exchange
    • The fees are not cheap – you probably won’t be happy with them
    • Then, use the money in your digital wallet like any other bank account
      • For places that take the specific cryptocurrency, that is

• A miner has an initial outlay of several thousands of dollars to buy a special computer, and then will spend hundreds of dollars a month for electricity to run it
  • But a miner might be able to generate (mine) their own money, rather than having to buy it
Where Are We?

- What is a blockchain?
- How are blockchains related to Bitcoin?
- How to use a cryptocurrency
- Using a blockchain for document protection
  - What types of problems or disputes can be addressed?
  - When should you consider using a blockchain?
- What parts of a blockchain do you really need?
- What does it look in operation?
- Example of using a blockchain to detect a forgery
Can **You** Use a Blockchain to Add Value for Clients?

- Likely, **YES**, if your work product includes documents that may be subject to dispute, later
- A blockchain can enhance the trustworthiness of a legally-significant document by enabling:
  - Easy proof, at a later time, that a particular document had both:
    1. Existed no later than a particular date when it was “put” into a blockchain (which may have been many years prior to when it is being challenged)
    2. And **has not been altered** since that date
  - If you can, watch the movie *Changing Lanes*, to learn about an interesting forgery risk
    - If, in the storyline, the court system had required that certain legal documents be put into blockchains, the document (that one of the characters submitted as a purportedly true copy) would have been immediately identifiable by the judge as a forgery
  - The ability to easily identify forgery attempts, even when the person who signed the real document is unavailable (such as, they are deceased) has obvious benefits
    - Eventually, court systems may encourage certain documents be put into a blockchain, by easing authentication of evidence in some situations when a witness is unavailable
  - See Federal Rules of Evidence (FRE) 901 (which is relevant to many lawsuits)
    - Someday, this particular rule may be adapted to accommodate blockchains
Can **You** Use a Blockchain to Add Value for Clients?

Ever worry that something like this might happen?

<table>
<thead>
<tr>
<th>My copy of the will is the real one. I get all of the money.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO! My copy is the real one. I get all of the money.</td>
</tr>
</tbody>
</table>

This one represents an actual lawsuit between Paul Ceglia and Mark Zuckerberg in 2010:

<table>
<thead>
<tr>
<th>I own part of Facebook. You were hired to make it for me. This contract proves it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. That contract is forged. You only hired me to make something called StreetFax.</td>
</tr>
</tbody>
</table>

Do you see a role for a blockchain in either of these scenarios?
Can *You* Use a Blockchain to Add Value for Clients?

Do you see a role for a blockchain in either of these scenarios?

Any document that is confidential today, but may be needed to settle a later dispute (even if that doesn’t occur until years from now), may benefit from being “put” into a blockchain now.


The article also describes using blockchain registration as a whitelist for parental controls.

---

*Where’s my money?*

*You spent all of it, already.*

*No, I didn’t! Prove it.*

*You stole my trade secrets by hiring away my designer.*

*We were working on our own version of the same project for years. The dates on our documents prove it.*

*Liar! You back-dated those.*
Where Are We?

• What is a blockchain?
• How are blockchains related to Bitcoin?
• How to use a cryptocurrency
• Using a blockchain for document protection
• What parts of a blockchain do you really need?
  • Mining is expensive – for both the equipment and electricity
  • Is using a cryptocurrency blockchain really necessary?
• What does it look in operation?
• Example of using a blockchain to detect a forgery
What Parts of a Blockchain are Relevant to Documents?

- What parts of a blockchain are relevant to protection of legally-significant documents?
  
  1. Tokens – No. Not needed
  
  2. Ledger – Not as implemented in cryptocurrencies, but just a list of hash values
     
     Do not put confidential documents into a chain that others can read
     
     Instead, hash the documents and insert those digital fingerprints into a block
     
     This is the definition of “put” promised earlier; “check” is recalculating the hash
     
     This is called “off-chain storage”; the documents are stored privately, elsewhere
  
  3. Blockchain – Yes. This is the trust mechanism that will provide the proof, later
  
  4. Consensus – Not as implemented in cryptocurrencies; only just verification of no forgery
     
     A permissioning authority can grow the chain and the public can detect forgery attempts
     
     The permissioning authority needs to be trusted only to put a record into the chain
     
     If the permissioning authority refuses, it’s no problem. Just send it to another chain
  
  5. Mining – No. Not needed
  
  6. Independent, duplicated storage – Not needed if a physical record can prove dates
     
     The hash that chains the different blocks together can be published in a newspaper ad
What Parts of a Blockchain are Relevant to Documents?

Here is an example for a system that uses USA Today:

USA TODAY · THURSDAY, MARCH 19, 2009 · 7D

ANNOUNCEMENTS

4E60D4F9D103800931AD86827D52D
E7BFC614486A032DB7AA004A6D4C3
A4193EA0C717E7592CA7290A5DBA9
7888BAF5048E799D32C229009FA42
CF2899CC74B47B900040A817BF451
DCE73E6A28D036F266E693B000002
090310a PEDDaL.com
What Parts of a Blockchain are Relevant to Documents?

• Some quick comments on why consensus may not be needed for document integrity proof.
• The purpose of consensus is to compensate for the fact that no one is in charge of managing the chain.
  • Why isn’t anyone managing cryptocurrency blockchains?
    • Because the designers of many current cryptocurrency systems wished to avoid (as best they could) the ability of governments to influence the currency or accounts.
    • If there was someone, a government could coerce that person to deny transactions.
  • Without a manager, who decides whether a particular block is added?
    • The solution: a vote of all community participants.
      • And then just hope the Chinese, Russians, Iranians, and North Koreans can’t control the voting by using their governments’ resources to build large numbers of systems.
• What about lawyers, banks, CPAs, large companies, … ?
  • People in these professions have submitted to government regulations and controls, so there’s no need to avoid a central manager.
• For blockchains used by regulated industries, a permissioning authority may be preferable.
  • A permissioning authority can monetize the chain by selling rights to submit document records, as well as limit participation to ease storage burdens and reduce legal risks.
What Parts of a Blockchain are Relevant to Documents?

- Some quick comments on why mining may not be needed for document integrity proof
- The purpose of mining is also to compensate for lack of a central chain manager
  - If blocks are added as quickly as votes can be taken, the chain will grow uncontrollably
  - Without a manager, who decides when a particular block is added?
    - The solution: before a new block can be proposed for voting, someone must solve a math problem that takes several minutes – even on a very fast computer
      - Blocks cannot be added more quickly than the math problem can be solved
  - The generation of tokens was a side benefit to slowing down the rate of the chain growth
    - Since tokens are not needed for document integrity proof, mining is unnecessary

- So, … consensus and mining are compensations for the lack of a central manager
  - Consensus is for whether a block is to be added
  - Mining is for when a block is to be added
  - Neither is needed for document integrity proof in regulated industries, when a permissioning authority controls the growth of the blockchain
Where Are We?

- What is a blockchain?
- How are blockchains related to Bitcoin?
- How to use a cryptocurrency
- Using a blockchain for document protection
- What parts of a blockchain do you really need?
- What does it look in operation?
  - A system for protecting legally-significant documents
  - Without the distraction of a cryptocurrency
  - Example of using a blockchain to detect a forgery
How to protect documents?

• Safe solution:
  Industry-specific blockchains accept submissions from industry participants and contain mostly hash values, rather than actual document contents
  • This drastically eases storage burdens in comparison with an uncontrolled participation
  • This can decrease the risk of legal issues, improving long-term viability

Researchers Discover Child Pornography Hidden in Bitcoin’s Blockchain
  March 21, 2018

Opinion: Bitcoin’s Biggest Problem Isn’t Child Porn, It’s GDPR
  March 31, 2018

Is Blockchain Incompatible With GDPR?
  April 10, 2018
How to protect documents?

Uncontrolled mob throws all sorts of documents at chain

Permissioning Authority accepts hash values from mainly legal industry

Long-term viable blockchain

Uncontrolled mob throws all sorts of documents at chain

Permissioning Authority accepts hash values from mainly financial industry

Long-term viable blockchain

Same for other industries: medical, real estate, manufacturing, travel, …

Make sense so far?
Permissioned Blockchains for Document Protection

• A permissioning authority adds value by improving long-term viability for blockchains used to prove age and integrity of legally-significant documents
  • Reasons that cryptocurrencies avoid permissioning authorities (in favor of consensus) are mostly inapplicable to industries such as legal, financial, manufacturing, and health care
• A permissioning authority can insulate a blockchain from certain problems:
  • Enforcing a hash-only policy has multiple benefits
    1. Precludes risk of the chain being banned over the presence of indecent material
    2. Precludes risk of the chain being banned for privacy issues (GDPR’s Right of Erasure)
    3. Prevents bloat, because hashes are (typically) shorter than the documents they protect
      • Burdensome storage demands might otherwise drive away community members
  • Limiting community membership has multiple benefits
    4. Further reduces bloat, when participation is limited to qualified industry participants
    5. The chain can be monetized by selling submission rights
      • Subscription model: Companies can protect some number of documents per month
      • Per-submission model: Low-volume or infrequent users pay a per-submission rate
• A system of this type has been operating since 2009 (See the earlier newspaper ad date)
Where Are We?

- What is a blockchain?
- How are blockchains related to Bitcoin?
- How to use a cryptocurrency
- Using a blockchain for document protection
- What parts of a blockchain do you really need?
- What does it look in operation?
- Example of using a blockchain to detect a forgery
  - Alice’s Will
Example: Detecting Forgery in Alice’s Will

- Alice created a 5 page Will with the following text:
  - Page 1: Last Will and Testament of Alice
  - Page 2: Second page.
  - Page 3: I give Bob $1,000,000.00 (One Million Dollars). I give Eve $1.00 (One Dollar).
  - Page 4: Fourth page.
  - Page 5: Notarized page
- The SHA-1 hash is: AB1A8C358166198D272F0260A2ECCE8FFD27CA8B
- Alice’s lawyer enters this hash into a blockchain, along with the lawyer’s digital signature
  - Alice also sends a letter to her heirs that her will has that specific hash value
  - But yet, even though everyone knows the hash value, they still don’t know the contents
- Years later, Eve finds a copy and creates a forgery with a different Page 3:
  - Page 3: I give Eve $1,000,000.00 (One Million Dollars). I give Bob $1.00 (One Dollar).
  - During probate, both of the versions are hashed
- Eve’s version SHA-1 is: 9D889BB550B8FC1B17BB6F0F0DA3D1B3AA31DC88
- Which one will be accepted as authentic?
If you have any further questions, send me an email
Kelce S. Wilson, JD, MBA, PhD
CIPP/US, CIPP/E, CIPM, USPTO-registered patent attorney
Use either of:
kwilson <at> softwareipattorney <dot> com;
questions <at> peddal <dot> com.
Kelce S. Wilson  
Attorney  
PEDDaL

Kelce Wilson was in the U.S. Air Force, active duty 1989-2002, then the reserves until 2010, reaching the rank of Lieutenant Colonel. He has a B.S., M.S. and Ph.D. in electrical engineering, an M.B.A., a J.D., and U.S. Patent and Trademark Office patent practitioner registration. Additionally, he is a certified privacy professional, with CIPP-US, CIPP-E, and CIPM. During his military and engineering career he worked in satellite control, cryptography, radar, jammers, stealth aircraft, automatic target recognition, surveillance radar, and cybersecurity testing. Mr. Wilson won the 2004 “Reservist of the Year” in Air Force Aeronautical Systems Center for solving multiple challenging mathematical problems that had been delaying development of stealth and radar jamming systems. In 2005, he received the Director’s Commendation from the National Geospatial-Intelligence Office for his contribution to measurement and signature intelligence (MASINT) workforce education.