Distributed Ledger Technologies

What are they and How could we use them?

Prepared by

Raul Cova

Distributed Ledger Technologies (DLT)

Secure | https://globalpetroleumshow.com/conference/

Stay up-to-date with the latest news from Global Petroleum Show | Get Updates!

Global Petroleum Show prides itself in being the **most important energy event** in North America attracting thousands of global thought leaders and influencers from countries around the world – **this year GPS celebrates its 50th anniversary.**

Over the past 50 years, learnings, new advancements, and technologies have been driving the evolution of the industry and in 2018, GPS will launch a comprehensive three-day business and technical conference to provide a high-level platform to share and discuss these revolutions. Each day of the GPS Conference includes a variety of business debates, panel discussions, high-level keynotes, and technical presentations.

The GPS Conference has been developed to answer three topical theme questions:

- How are traditional oil & gas companies forging ahead in a transformed global energy landscape?
- How are companies in all energy sectors diversifying their portfolios to support future sustainability and environmental implications?
- How are digital systems, such as Blockchain, changing the way companies and countries do business?

ALBERTA INNOVATES · BAKER HUGHES a GE company · cenovus ENERGY · Chevron · Canadian Natural · devon

GLOBAL PETROLEUM SHOW

North America's Leading Energy Event
June 12 - 14, 2018
Stampede Park
Calgary, Canada

The GPS Conference has been developed to answer three topical theme questions:

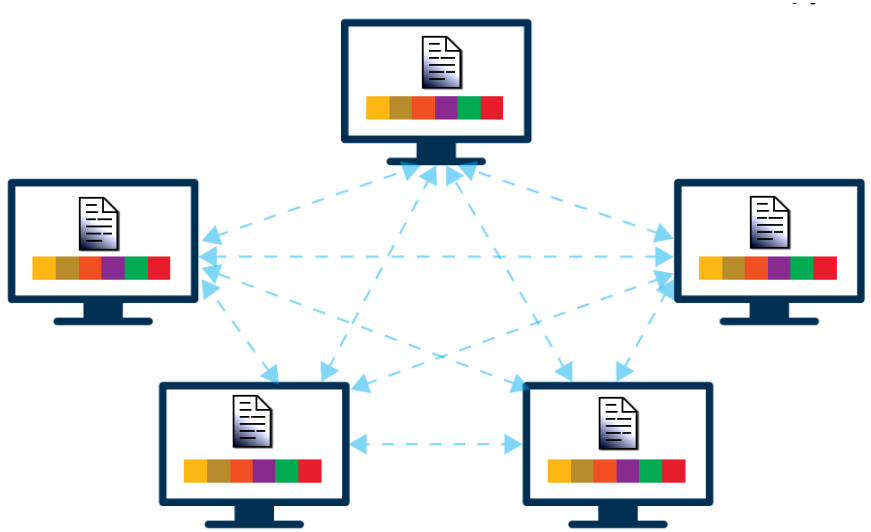
- How are traditional oil & gas companies forging ahead in a transformed global energy landscape?
- How are companies in all energy sectors diversifying their portfolios to support future sustainability and environmental implications?
- How are digital systems, such as Blockchain, changing the way companies and countries do business?

Distributed Ledger Technologies (DLT)

- DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers).

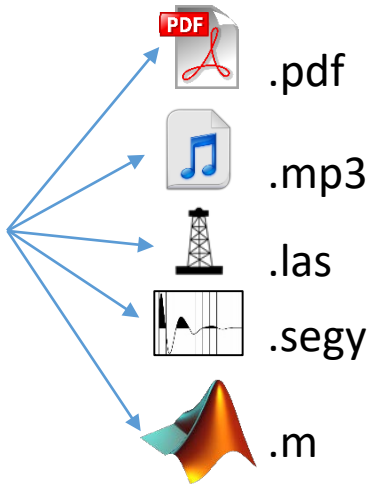
- This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants.

  - Blockchains
  - Smart contracts
  - Chainless technologies
    - IoT: Directed Acyclic Graphs (DAG)



Distributed ledger

- An asset database that can be shared across a network of multiple sites, geographies or institutions.
  - Assets can be financial, legal, physical or electronic.



- Properties
  - Cryptography is used to manage the ledger in a secure way
  - Immutable: once an entry is recorded in the database it is extremely difficult to be altered.
  - Tamper evident: if a record is changed the network can detect it immediately.
  - Decentralized: No need for a central authority to enforce the rules (*"In code we trust")*

  By having a large distributed network of independent users, data integrity can be maintained without the need for a central authority

Blockchain

- “Cryptographically secured” data structure consisting of blocks, time stamps and transaction data linked in a chain.
- A record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network.
- The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset.

Blockchain

- Blocks hold batches of valid data that are hashed and encoded into a Merkle tree.
- Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain.
- This iterative process secures the integrity of the previous block, all the way back to the original genesis block.

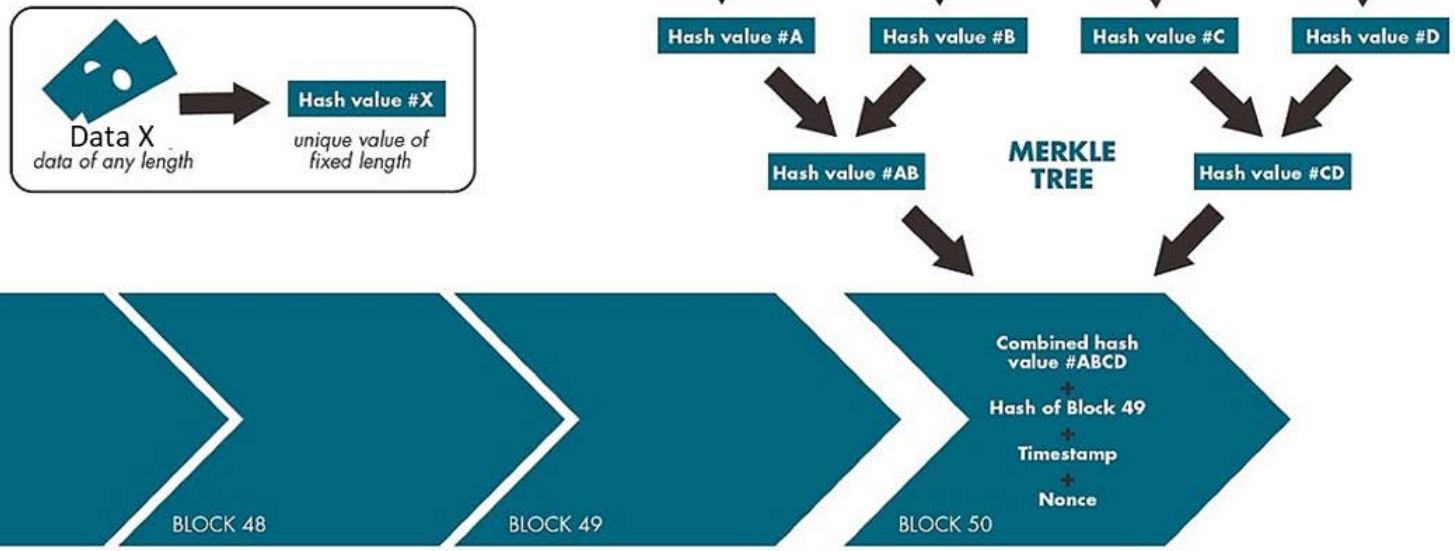


Figure adapted from: “The Great Chain of Being Sure About Things” by The Economist

Hash functions

A function that takes an input of any size and returns an output with a fixed size.

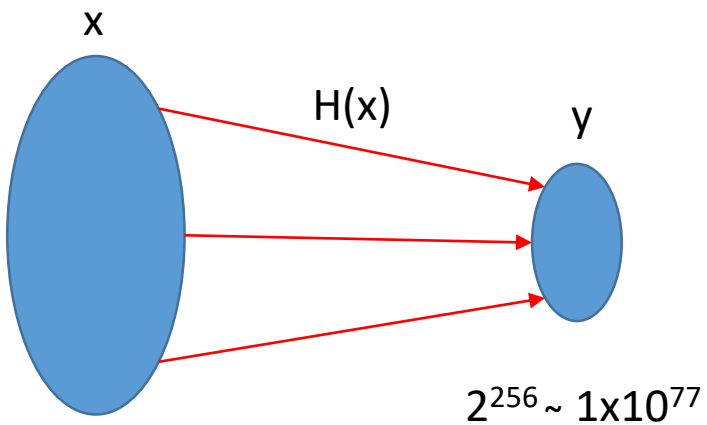
- SHA256 outputs strings that are 256 bits long.

Properties:

- Collision free: No body can find x and y such that for x!=y we obtain H(x) = H(y).

- Hiding: Given H(r|x), with r chosen from a very spread out distribution, it is infeasible to find x.

- Puzzle-friendly: Given H(id|x) ϵ Y, no solving strategy for x is much better than trying random values of x.



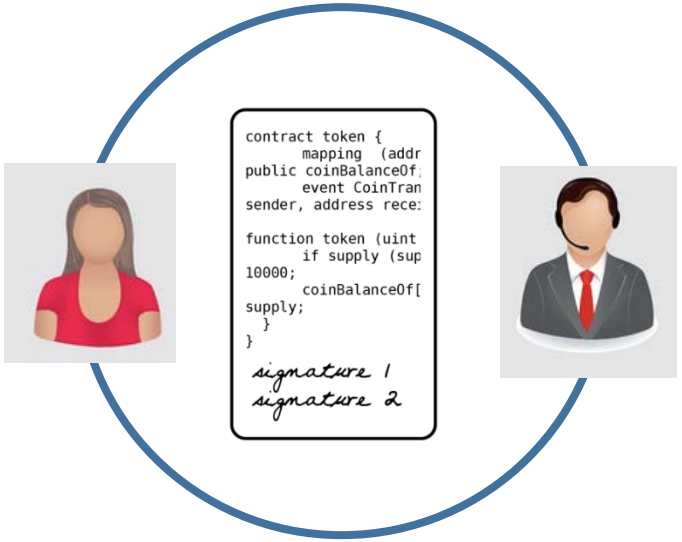
$2^{256} \sim 1x10^{77}$

SHA256('CREWES')= 85f0e143ecf66a98c2a01173df36c02e3d27940a120974a6dca52e9df02e5bb8

Smart contracts

- Blockchain-based smart contracts are contracts that can be partially or fully executed or enforced without human interaction.

  e.g. creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level.

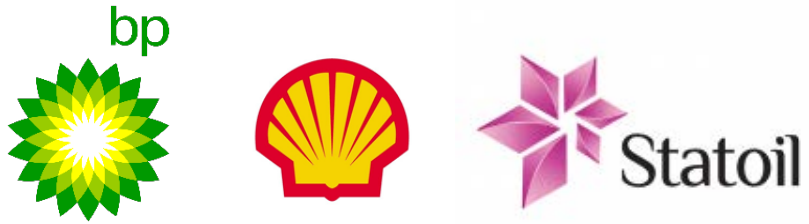


- Smart contracts go beyond transactions and enable exchange of value or information without powerful intermediaries acting as arbiters.

Trading and tracking oil shipments

- Problem: Title transfers and post trades are heavy on paperwork.
- Even though each party could keep digital records of their operations, using a distributed ledger will force buyers and seller to use the same record book.
- Using a blockchain provides a secure way of recording deal histories that can be accessible to the network users.
- Disclosing asset custody within a blockchain, makes clear to everyone who owns what and where the assets came from.

Oil producers

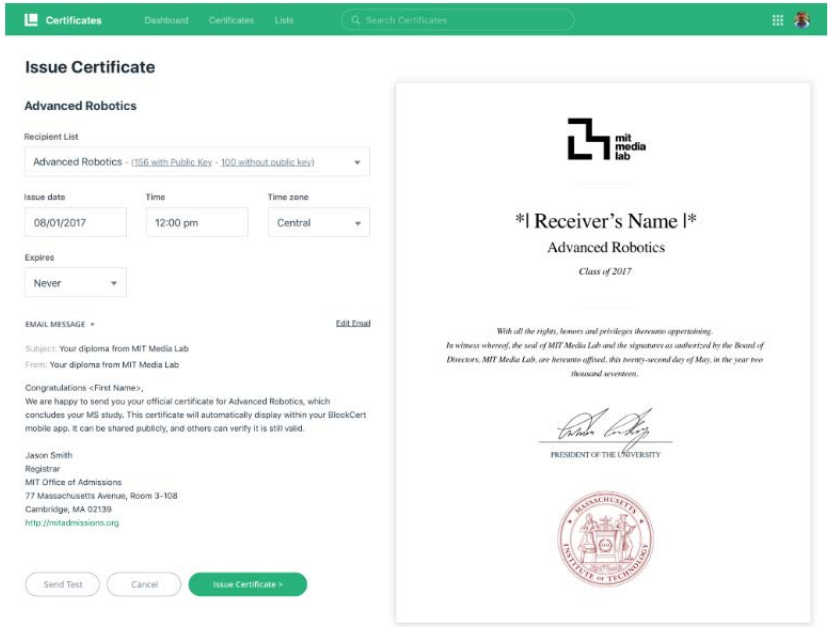


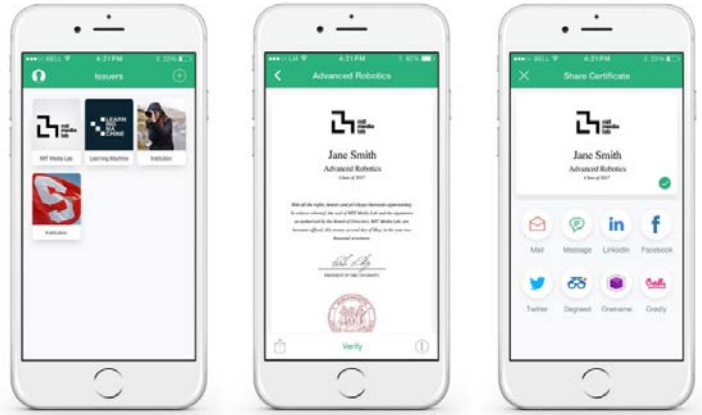
Commodity traders

Lenders

Certifying academic records

- The Digital Certificates Project at MIT has been developing an ecosystem for creating, sharing and verifying blockchain-based educational records.
- Make tamper-proof academic records available to anyone at any time.



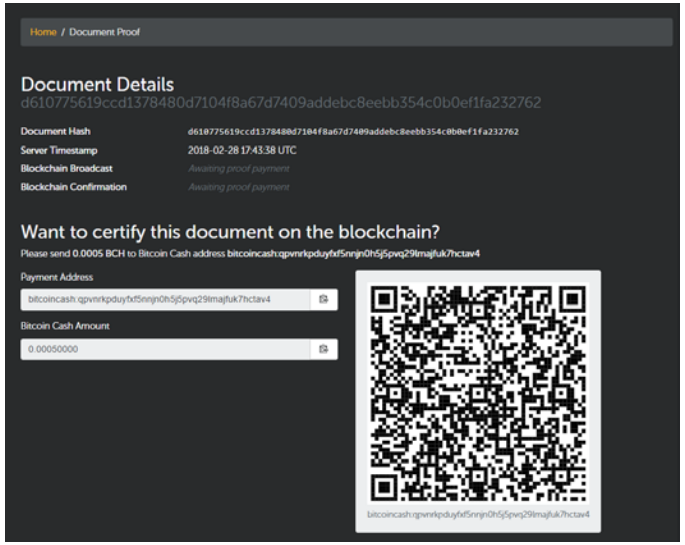


Figures from: https://medium.com/learning-machine-blog/why-the-blockchain-will-revolutionize-academic-credentialing-9950c9c4928d

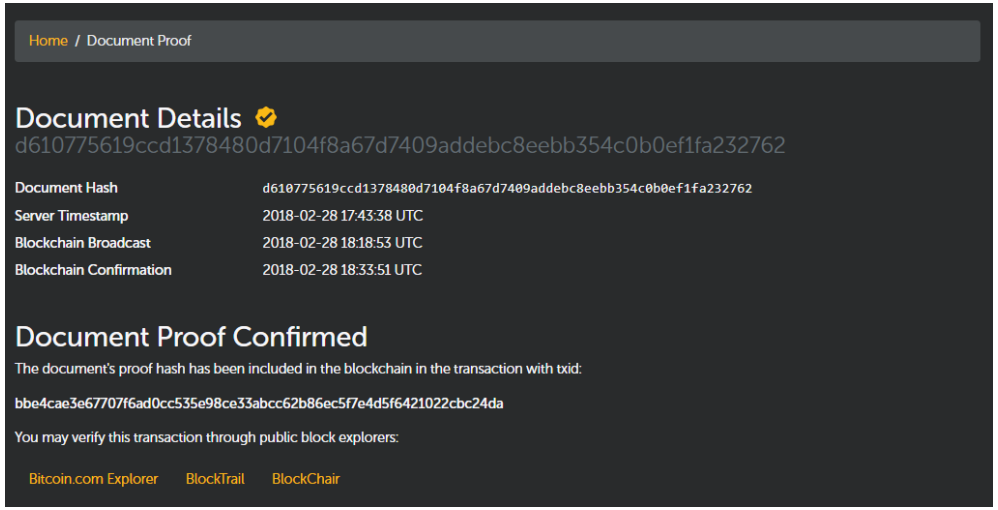
Notarizing CREWES reports

Just for fun!

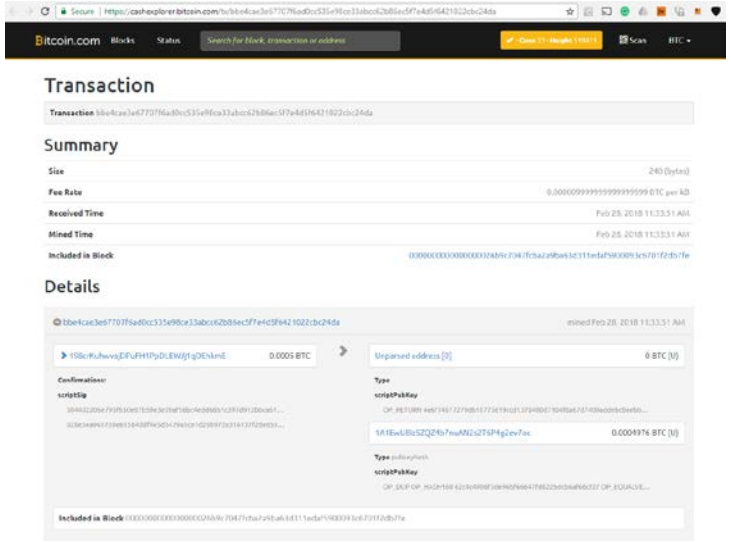
Compute hash of the document, time-stamp it and broadcast it to the bitcoin network



Copies of the document can be verified now against the record in the blockchain



Details about the transaction, like cryptographic signatures, can be seen on any public blockchain explorer



Certifying .las and .segy files

- Problem: validating the source of a .segy or .las file
  - A secured record of acquired well logs and seismic data and their metadata could be maintained.
  - Data do not need to be shared with the network. Only their hashes and a hash table with pointers to a private database are needed to maintain the records. Metadata can be included in the blockchain to facilitate search and data validation.
  - A public permissioned blockchain may achieve this goal.

Auditing processing jobs

- Problem: validating processing flows applied on seismic data
  - The hash of the output of a processing step along with the parameters used in the processing can be registered in a distributed ledger facilitating audits through the processing sequence.
  - An smart contract could be set up such that invoices are automatically generated at every processing step.
  - Companies could include a set of required processing parameters within the smart contract. Invoices will only be produced if the required parameters were used in the processing sequence.

Thanks !