UNIT 2 BCT - block chain technology

COMPUTER SCIENCE ENGINEERING (Jawaharlal Nehru Technological University, Kakinada)

<u>**UNIT 2**</u>

Hashing Data Structure

What is Hashing?

Hashing is a technique or process of mapping keys, and values into the hash table by using a hash function. It is done for faster access to elements. The efficiency of mapping depends on the efficiency of the hash function used.

Let a hash function H(x) maps the value x at the index x%10 in an Array. For example if the list of values is [11, 12, 13, 14, 15] it will be stored at positions {1, 2, 3, 4, 5} in the array or Hash table respectively.

What is Hashing in Blockchain?

A hash function is a mathematical function that takes an input (which can be of any size) and produces a fixed-length output, typically represented as.. Read More. However, the hash value itself is not an encryption of the input data, but rather a unique representation of it.

Blockchain Hash Function

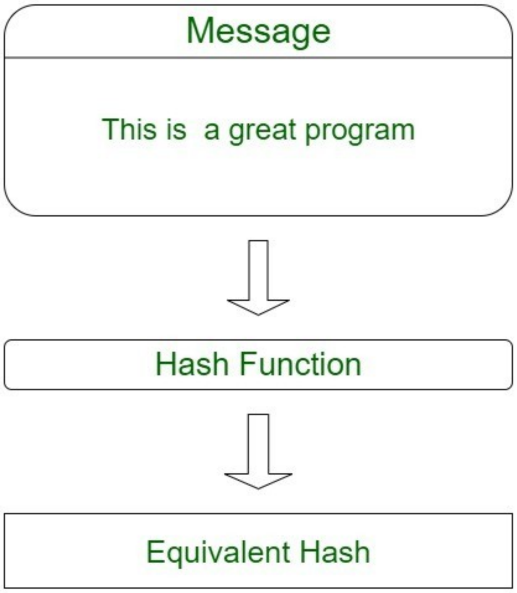
A hash function is a mathematical function that takes an input string of any length and converts it to a fixed-length output string. The fixed-length output is known as the hash value. To be cryptographically secure and useful, a hash function should have the following properties:

- ✓ **Collision resistant:** Give two messages m1 and m2, it is difficult to find a hash value such that hash(k, m1) = hash(k, m2) where k is the key value.
- ✓ **Preimage resistance:** Given a hash value h, it is difficult to find a message m such that h = hash(k, m).
- ✓ **Second preimage resistance:** Given a message m1, it is difficult to find another message m2 such that hash(k, m1) = hash(k, m2).
- ✓ **Large output space:** The only way to find a hash collision is via a brute force search, which requires checking as many inputs as the hash function has possible outputs.
- ✓ **Deterministic:** A hash function must be deterministic, which means that for any given input a hash function must always give the same result.
- ✓ **Avalanche Effect:** This means for a small change in the input, the output will change significantly.
- ✓ **Puzzle Friendliness:** This means even if one gets to know the first 200 bytes, one cannot guess or determine the next 56 bytes.
- ✓ **Fixed-length Mapping:** For any input of fixed length, the hash function will always generate the output of the same length.

How do Hash Functions work?

The hash function takes the input of variable lengths and returns outputs of fixed lengths. In cryptographic hash functions, the transactions are taken as inputs and the hash algorithm gives an output of a fixed size.

The below diagram shows how hashes work.

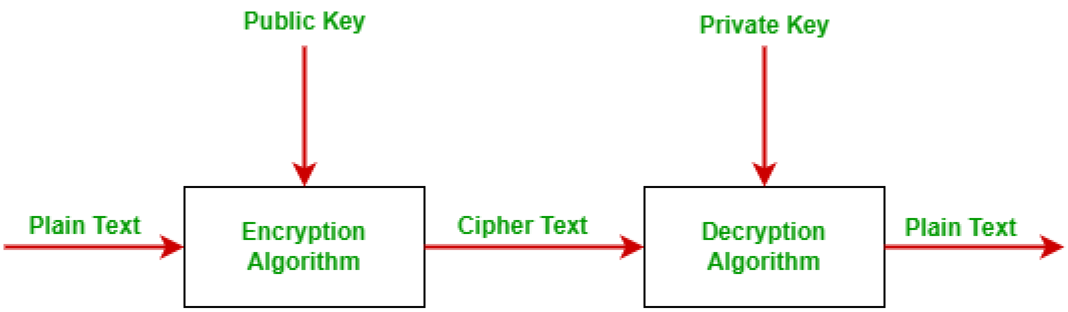


Blockchain – Public Key Cryptography

Blockchain technology is one of the greatest innovations of the 21st century. In this article, we will focus on the concept of cryptography i.e. public-key cryptography or Asymmetric key cryptography.

Introduction To Public-Key Cryptography

Most of the time blockchain uses public-key cryptography, also known as asymmetric-key cryptography. Public key cryptography uses both public key and private key in order to encrypt and decrypt data. The public key can be distributed commonly but the private key can not be shared with anyone. It is commonly used for two users or two servers in a secure way.



Public Key: Public keys are designed to be public. They can be freely given to everyone or posted on the internet. By using the public key, one can encrypt the plain text message into the cipher text. It is also used to verify the sender authentication. In simple words, one can say that a public key is used for closing the lock.
Private Key: The private key is totally opposite of the public key. The private key is always kept secret and never shared. Using this key we decrypt cipher text messages into plain text. In simple words, one can say that the private key is used for opening the lock.

Blockchain public vs private and use cases

Unlike public blockchains like Bitcoin or Ethereum, where anyone can participate and transactions are transparent to everyone, private blockchains have restricted access and provide more control and privacy to the network participants.

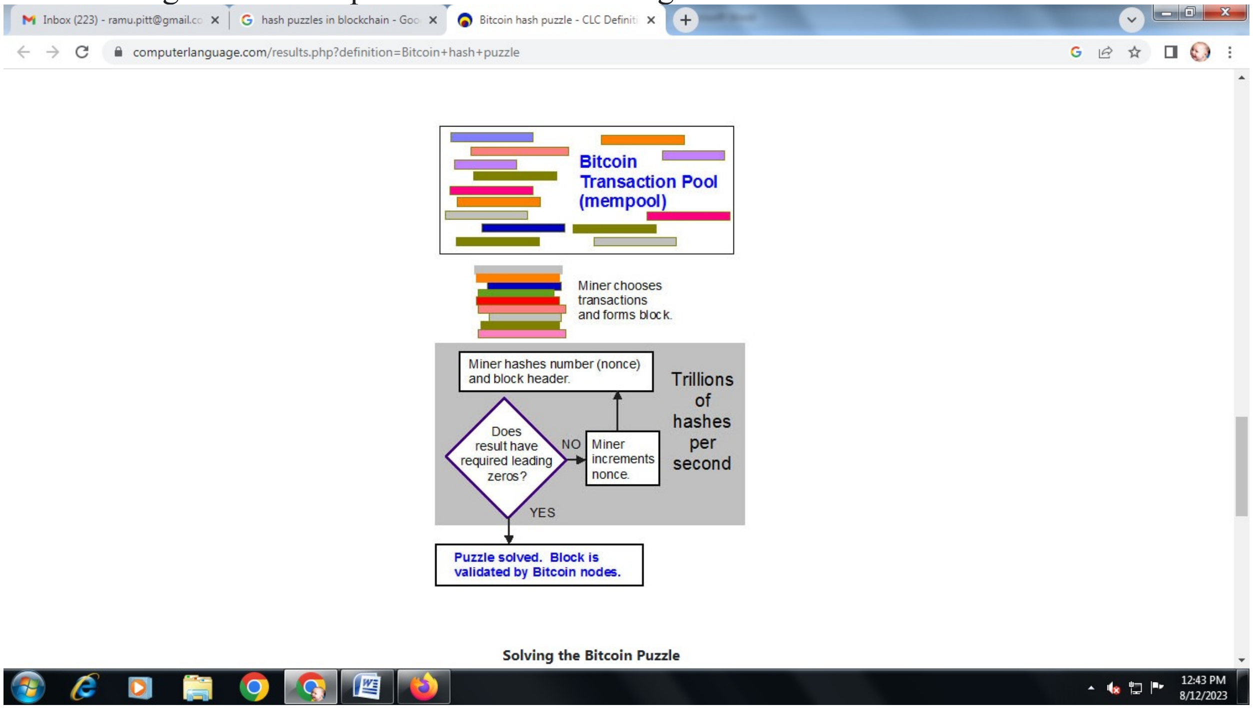
Difference between Public and Private blockchain :

S.no	Basis of Comparison	PublicBlockChain	Private BlockChain
1.	Access –	In this type of blockchain anyone can read, write and participate in a blockchain. Hence, it is permissionless blockchain. It is public to everyone.	In this type of blockchain read and write is done upon invitation, hence it is a permissioned blockchain.
2.	Network Actors –	Don't know each other	Know each other
3.	Decentralized Vs Centralized –	A public blockchain is decentralized.	A private blockchain is more centralized.
4.	Order Of Magnitude –	The order of magnitude of a public blockchain is lesser than that of a private blockchain as it is lighter and provides transactional throughput.	The order of magnitude is more as compared to the public blockchain.
5.	Native Token –	Yes	Not necessary
6.	Speed –	Slow	Fast
7.	Transactions pre second –	Transactions per second are lesser in a public blockchain.	Transaction per second is more as compared to public blockchain.
8.	Security –	A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for 'bad actors' to attack the system and gain control over the consensus network.	A private blockchain is more prone to hacks, risks, and data breaches/ manipulation. It is easy for bad actors to endanger the entire network. Hence, it is less secure.
9.	Energy Consumption –	A public blockchain consumes more energy than a private blockchain as it requires a significant amount of electrical resources to function and achieve network consensus.	Private blockchains consume a lot less energy and power.

10.	Consensus algorithms –	Some are proof of work, proof of stake, proof of burn, proof of space etc.	Proof of Elapsed Time (PoET), Raft, and Istanbul BFT can be used only in case of private blockchains.
11.	Attacks –	In a public blockchain, no one knows who each validator is and this increases the risk of potential collision or a 51% attack (a group of miners which control more than 50% of the network's computing power.).	In a private blockchain, there is no chance of minor collision. Each validator is known and they have the suitable credentials to be a part of the network.
12.	Effects –	Potential to disrupt current business models through disintermediation. There is lower infrastructure cost. No need to maintain servers or system admins radically. Hence reducing the cost of creating and running decentralized application (dApps).	Reduces transaction cost and data redundancies and replace legacy systems, simplifying documents handling and getting rid of semi manual compliance mechanisms.
13.	Examples –	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.	R3 (Banks), EWF (Energy), B3i (Insurance), Corda.

Hash puzzles in blockchain

The puzzle is finding the random number that, when added to the block's header, generates a hash with some number of leading zeros. Trying a new number trillions of times per second, the miner algorithm attempts to find the one that generates the desired results.


Inbox (223) - ramu.pitt@gmail.co
hash puzzles in blockchain - Goo
Bitcoin hash puzzle - CLC Definiti
computerlanguage.com/results.php?definition=Bitcoin+hash+puzzle
Bitcoin Transaction Pool (mempool)
Miner chooses transactions and forms block.
Miner hashes number (nonce) and block header.
Trillions of hashes per second
Does result have required leading zeros?
NO
Miner increments nonce.
YES
Puzzle solved. Block is validated by Bitcoin nodes.
Solving the Bitcoin Puzzle
12:43 PM
8/12/2023

6 Essential Blockchain Technology Concepts You Need To Know

1. Blockchain and Bitcoin are not the same

Many people assume that blockchain and bitcoin are the same. Blockchain is the underlying technology of Bitcoin. They are closely related, but they are not the same thing.

In 2008, Bitcoin was introduced as a type of unregulated digital currency created by the pseudonymous Satoshi Nakamoto. Blockchain was the ledger solution used to securely record facilitating the use of this new currency since there was no bank or government involved to monitor or police the transactions. As such Bitcoin can actually be considered as the first use case leveraging blockchain technology. The confusion between blockchain and bitcoin often arises because these two concepts were introduced at the same time.

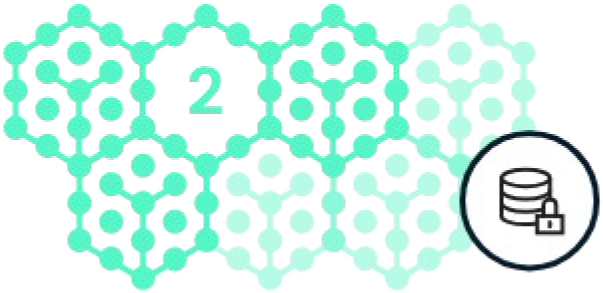
Blockchain and Bitcoin transactions

Since the introduction of blockchain technology it has been extrapolated for use as a ledger solution in many other industries related to assets other than a currency. These fields include healthcare with patient records, trade finance and owner of an invoice or purchase order, as well as insurance and who has the title to a house or car.

Bitcoin is known as a cryptocurrency and the first decentralised digital currency of its kind. It was launched as an open-source solution to work without a central repository or single administrator. Bitcoin transactions are transferred and saved using a distributed ledger on a shared network that is open, public and anonymous. Blockchain is the underlying technology that maintains the transaction ledger for Bitcoin transactions.

The blockchain technology as for example the one used for Bitcoin allows for the recording of transactions on a distributed ledger across a network of users. The open-source technology allows for the storage of data from the transactions into blocks. Each block includes a time-stamped record of the transactions with each block linked to the previous one, thus creating a chain. The information stored on the blockchain is fully transparent and permanent without the ability to change or remove previous transaction data from the distributed ledger. This characteristic and solution can be used to solve many inefficiencies in different applications and industries.

Whilst blockchain is an excellent choice for a digital currency, it can be used to keep a trusted audit train of ownership of a vast range of asset types. These can be both intangible (e.g. trade finance assets) and tangible (e.g. diamonds) assets. This makes for a highly diverse choice of blockchain applications for multiple sectors and institutions – including Marco Polo Network (formerly known as TradeIX) focusing on the trade finance industry with dedicated solutions leveraging blockchain technology.



2. Data stored on blockchain is public

This statement is partially correct. Some public blockchain are open, though others are private accessible only to specified users. The use case will determine which type of blockchain is needed. There are basically three types of blockchains.

Public blockchains

In a public blockchain, a user can become a member of the blockchain network. This means they can store, send and receive data after downloading the required software on their device. Allowing anyone to read and write the data stored on the blockchain as it is accessible to everyone in the world.

A public blockchain is completely decentralised. The permissions to read and write data onto the blockchain are shared equally by all connected users, who come to a consensus before any data is stored on the database.

The most popular example of a public blockchain is Bitcoin. The digital currency allows users to use a platform for making transactions directly between them.

Private blockchains

In a private blockchain, permission to write, send and receive data is controlled by one organisation. Private blockchains are typically used within an organisation with only a few specific users allowed to access it and carry out transactions.

The organisation in control has the power to change the rules of a private blockchain and may also decline transactions based on their established rules and regulations.

An example of this is a blockchain deployed by a corporation to collaborate with other divisions or a few permissioned participants.

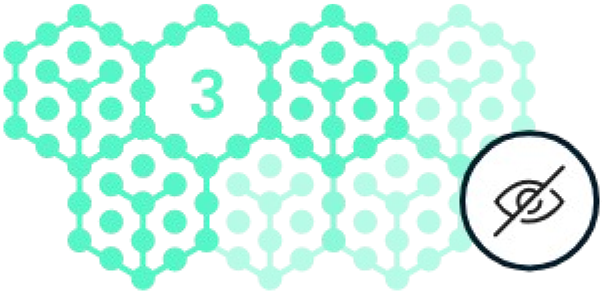
Consortium blockchains

A consortium blockchain, also called permissioned blockchain can be considered as a hybrid model between the low-trust offered by public blockchains and the single highly-trusted entity model of private blockchains. Instead of allowing any user to participate in the verification of the transaction process or on the other side just allowing one single company to have full control, in a consortium blockchain a few selected parties are predetermined. It only allows a limited number of users the permission to participate in the consensus process.

For example, imagine a group or network of ten banks, each of which is connected to the blockchain network. In this example, we could imagine that for a block to be valid, seven of the ten banks have to agree.

Although there is some degree of centralisation in this structure, users can grant permissions to read or write to other users. This leads to the partially decentralised design of consortium blockchains. Similar to private blockchains, the consortium blockchains keep the privacy of the data, without consolidating power within a single organisation.

An example of this is Marco Polo which is a banking initiative for trade finance powered by R3's blockchain technology.

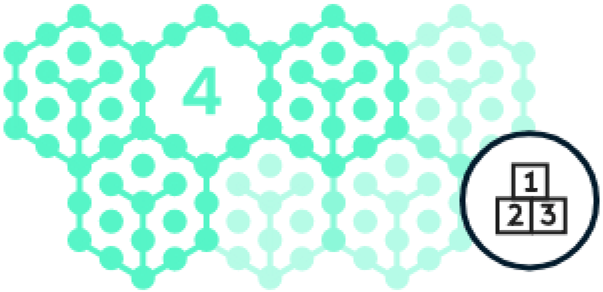


3. On the blockchain, private information is visible to everybody

People often think that all their information and transaction details posted on to the blockchain are public, based on the fact that the distributed ledger is public. This is not correct.

Though visibility depends on different use cases and the technology deployed. Narrowing the scope to this question – for business to business purposes, all transactions are private and only visible with the appropriate permissions. A company leveraging a blockchain to distribute data to their suppliers does not mean his competitors can see his suppliers or what they are buying. Nor can the suppliers see other suppliers' data. It is all private and secure and the suppliers only see the data the buyer has permissioned them to see.

Whilst some transactional information can be made public, what is stored on the distributed ledger is nothing more than the amount of the transaction and a hash. The hash is a code generated by running the actual transaction details through a cryptographic method. Therefore, it is impossible to have access to more information on the transaction.

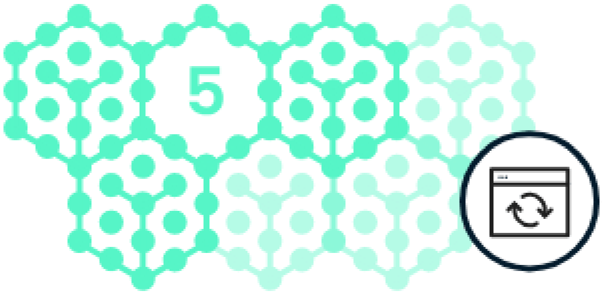


4. There is only one blockchain

The term blockchain is most often used to describe a ledger technology, not a specific product or solution. A blockchain solution will have the same common denominators such as being distributed and underpinned by cryptography and having some form of consensus mechanism.

However, there are various blockchains that come in public, permissioned or private versions. Today, there are dozens of different protocols, considered as blockchains and can be classified as distributed ledger technologies. For example Ethereum, Corda from R3, Fabric from IBM and Ripple.

Some are similar while others differ greatly from one another. Each blockchain solution will have specific advantages and disadvantages for the specific use, different use cases and applications.



5. Smart Contracts are legal documents

The term Smart Contract is misleading. They are neither “smart” nor a “contract” typically construed as legal document. Smart Contracts, which was first introduced as a term by cryptography researcher Nick Szabo in 1994 are basically scripts or software codes written by developers and deployed onto a blockchain. They are written as transaction instructions usually triggered by events. As an example, if goods arrive at this customer’s warehouse by this date, release payment to the supplier. Thus, automatically by companies updating shipments and receipts Smart Contracts can automatically perform tasks. This eliminates the need to manage time consuming and costly manual business processes.

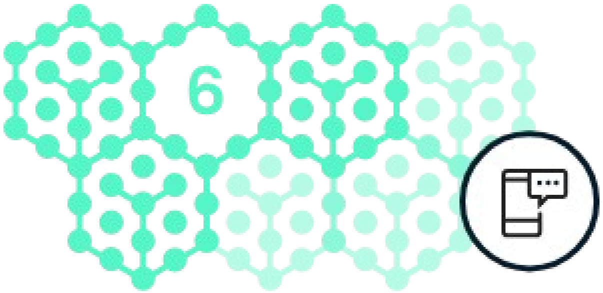
A smart-contract is a digital program that automates the execution of business logic, obligations, and agreements.

A smart-contract can be used to represent almost anything- an electronic warehouse receipt, a bond, an invoice, a unit of electricity, a unit of currency, a futures contract, a share of risk, and much more. These cryptographically unique assets can be created, traded, and settled in real time by users on the network. Each smart-contract can be written to include almost any type of business logic. This business logic can be enforced automatically in accordance with the terms and conditions of the agreement.

As inputs occur, the contract responds by executing any type of obligations or conditions mandated by the logic of the contract.

- a GPS coordinate indicating the arrival of a ship at the correct port could automatically trigger payment to the seller of goods carried by that ship.
- The input of the current price of a certain commodity could trigger the smart-contract to sell an option on that commodity.
- A buyer's signature on an invoice can create a payment obligation that is automatically executed on the date specified if and when other conditions are met.
- A vending machine can pay the drone who restocks it upon completion of the restocking and based on the inventory it has been stocked with,
- Collateral is transferred to creditor upon default event as received in court filing system.

As mentioned, Smart Contracts are typically not legal agreements. However, they can execute terms based on prior or separate agreements between parties. In addition, since legal agreements tend to follow a logical format such as if-this- then-that, similar to code, paper-based agreements could be replaced with computer-based programs which automatically execute the terms of a contract. Therefore, Smart Contracts play an important role in operating blockchain models. Specifically where processes between different parties can be automated by using automated rules, embedded smart contracts, thereby fulfilling the contractual intentions of parties with speed, clarity and efficiency.



6. Blockchain – a buzzword, nothing more

First blockchain is a real technology available today. Currently, blockchain is being tested with proof on concepts (POCs) in many different industries and regions around the world. Also keep in mind this is still early days for this technology. Several blockchain providers, like IBM and R3, released version 1 of their solutions in 2017. So, this is all very new and emerging right in front of us.

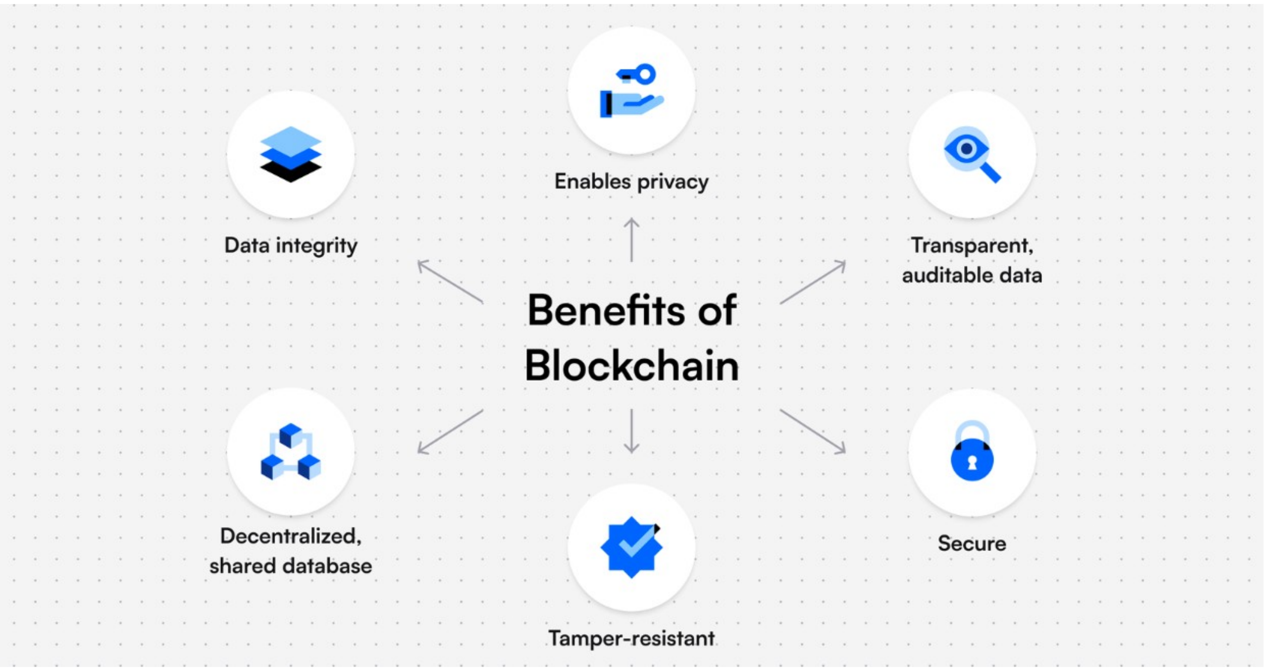
Indeed, blockchain has become arguably an overused term and covered daily in multiple media and press outlets. This does not mean that it is just a buzzword as the investment numbers speak for themselves.

In 2016, over $280 million was spent on blockchain technology by capital markets firms[1] with 90% of North American and European banks exploring blockchain solutions[2] During the same year, over $1.4 billion was invested globally in blockchain start-up companies.[3] Already today, approximately 50% of leading banks are working with a technology company to augment their blockchain capabilities.[4]

The investments in the technology and emerging companies are aligned with the potential efficiency gains for financial institutions. Accenture expects that more than $8 billion can be achieved in annual savings for the largest eight banks. By implementing blockchain technology there's potential for 70% in cost savings on business operations and 30-50% potential cost savings on compliance.

Digital identity verification in blockchain

What is digital identity verification in blockchain?



Secure identity verification: Digital identity systems leveraging blockchain can instantly and securely verify the identity and credentials of individuals for various purposes, such as opening bank accounts, or accessing government services.

Digital Identity Blockchain

At Dock, we built our own digital identity blockchain because it was:

- **Faster:** Other blockchain options were congested and took a long time to finalize transactions
- **Most cost-effective:** There weren't many good solutions at the time for making transactions

- **Customization:** Our public, permissionless blockchain is built specifically for decentralized identity use cases to better accommodate customers

- **Precedence:** We're a first class application on our own chain in contrast to other chains where we would run the risk of being preempted by other work

The Dock blockchain serves as a foundation of trust by keeping an authentic record of all verifiable DIDs, public cryptography keys, and invalidation registries.

Verifiable Credentials that are issued are stored outside of the chain, usually in a holder's digital wallet app, along with its corresponding cryptographic key pairs. To ensure data privacy, the only data entered on the Dock chain are the issuer's and holder's DIDs, Credential Schema (its "template"), and Revocation Registries.

Digital Identity Blockchain Examples

These are just a few of many examples of how Dock's digital identity blockchain can be leveraged in various industries:

- **Secure identity verification:** Digital identity systems leveraging blockchain can instantly and securely verify the identity and credentials of individuals for various purposes, such as opening bank accounts, or accessing government services. Blockchain-based identity verification provides enhanced security as it eliminates the need for centralized third-party verification services and prevents identity fraud and theft.
- **Healthcare Records:** Patients can create and manage their own digital identity while healthcare providers can securely verify patient records and medical histories. This can result in providing better care while also ensuring data privacy and security.

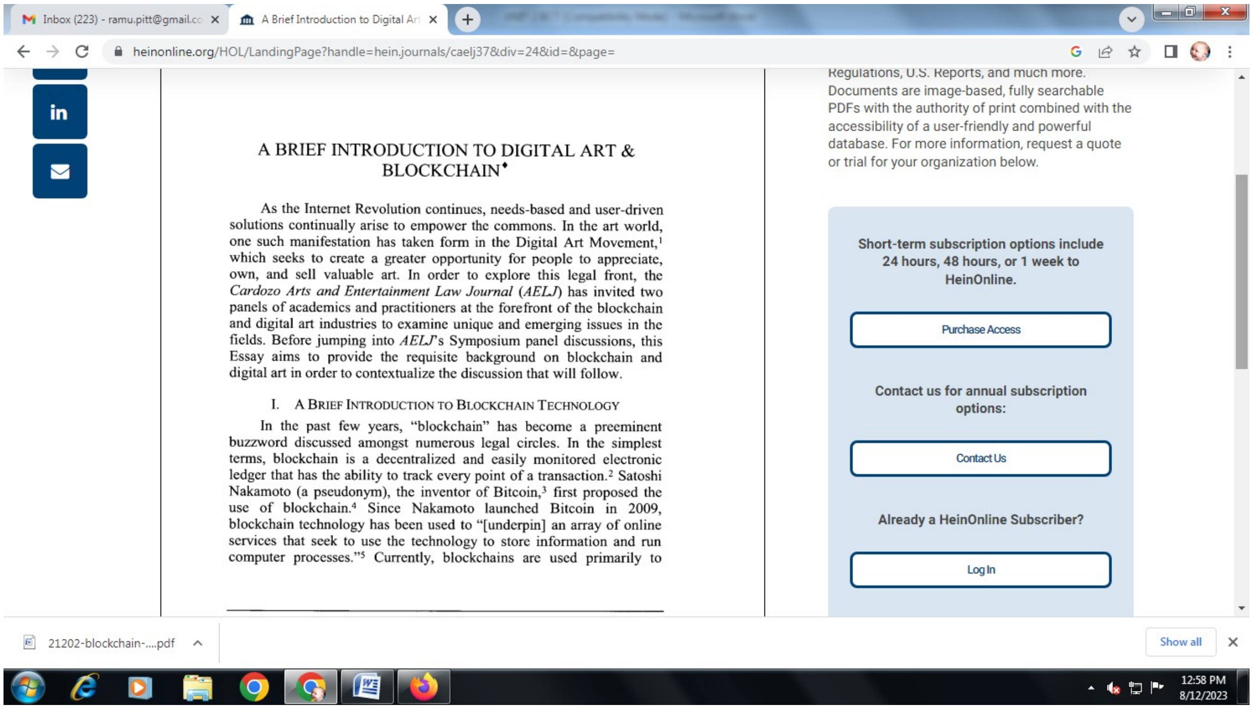
- **Supply Chain Management:** Blockchain-based digital identities can be used to track and manage supply chain information, providing greater transparency and security. By creating digital identities for products, supply chain managers can track the movement of goods across the supply chain, ensuring product authenticity and preventing counterfeiting and fraud.

Blockchain neutrality

The technology of blockchain is neutral in the system of artificial intelligence. This technology provides transparency in every sector where it has been used. Blockchain is used in many different sectors either in finance, Border control systems or in hospitals.

Neutrality of Blockchain Technology Creating Differences?

The technology of blockchain is neutral in the system of artificial intelligence. This technology provides transparency in every sector where it has been used. Blockchain is used in many different sectors either in finance, Border control systems or in hospitals. Nowadays mostly people aren't aware of this tech due to lack of understanding and skill and also because of different perceptions regarding the technology.


Inbox (223) - ramu.pitt@gmail.co
A Brief Introduction to Digital Ar
heinonline.org/HOL/LandingPage?handle=hein.journals/caelj37&div=24&id=&page=
21202-blockchain-....pdf
Show all
12:58 PM
8/12/2023

A BRIEF INTRODUCTION TO DIGITAL ART & BLOCKCHAIN♦

As the Internet Revolution continues, needs-based and user-driven solutions continually arise to empower the commons. In the art world, one such manifestation has taken form in the Digital Art Movement,[1] which seeks to create a greater opportunity for people to appreciate, own, and sell valuable art. In order to explore this legal front, the *Cardozo Arts and Entertainment Law Journal* (*AELJ*) has invited two panels of academics and practitioners at the forefront of the blockchain and digital art industries to examine unique and emerging issues in the fields. Before jumping into *AELJ*'s Symposium panel discussions, this Essay aims to provide the requisite background on blockchain and digital art in order to contextualize the discussion that will follow.

I. A BRIEF INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

In the past few years, "blockchain" has become a preeminent buzzword discussed amongst numerous legal circles. In the simplest terms, blockchain is a decentralized and easily monitored electronic ledger that has the ability to track every point of a transaction.[2] Satoshi Nakamoto (a pseudonym), the inventor of Bitcoin,[3] first proposed the use of blockchain.[4] Since Nakamoto launched Bitcoin in 2009, blockchain technology has been used to "[underpin] an array of online services that seek to use the technology to store information and run computer processes."[5] Currently, blockchains are used primarily to

Regulations, U.S. Reports, and much more. Documents are image-based, fully searchable PDFs with the authority of print combined with the accessibility of a user-friendly and powerful database. For more information, request a quote or trial for your organization below.

Short-term subscription options include 24 hours, 48 hours, or 1 week to HeinOnline.

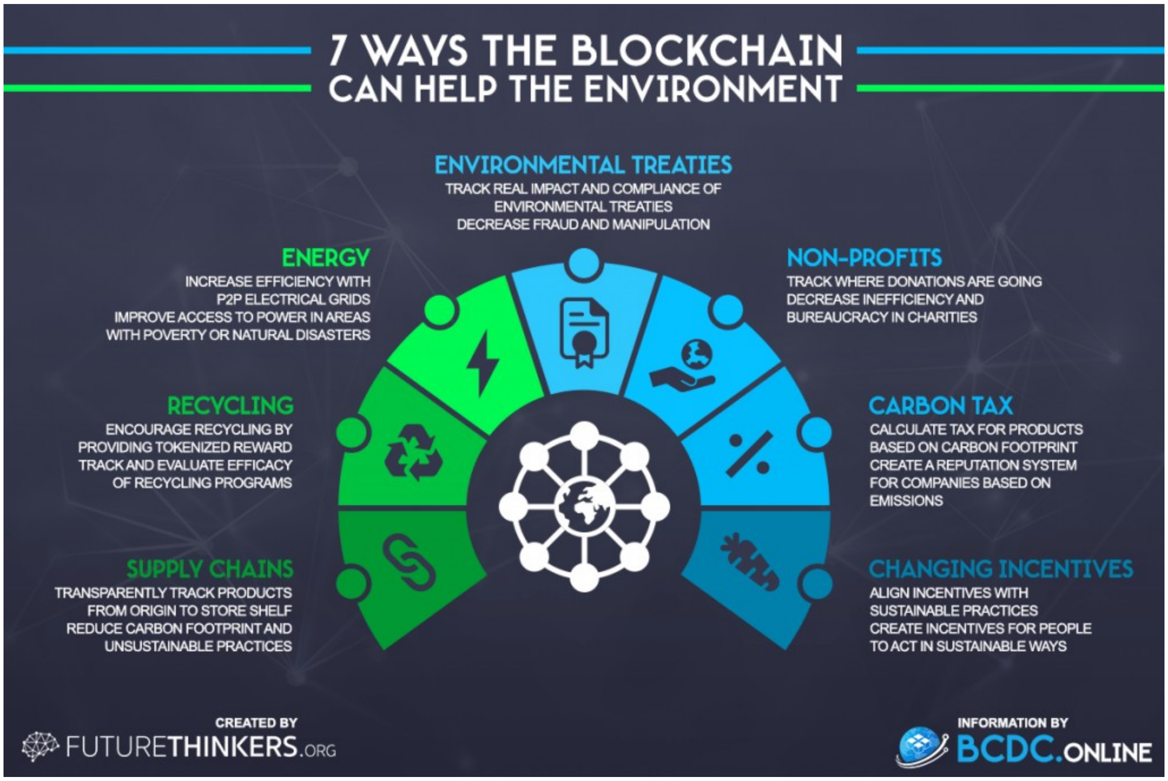
Contact us for annual subscription options:

Already a HeinOnline Subscriber?

Block chain environment

Blockchain can be used to provide transparency in supply chains, which can help identify and reduce environmental impacts. For example, blockchain can be used to track the origin of products and ensure that they are produced in an environmentally sustainable way.

How blockchain can protect the environment?



7 WAYS THE BLOCKCHAIN CAN HELP THE ENVIRONMENT

ENVIRONMENTAL TREATIES
TRACK REAL IMPACT AND COMPLIANCE OF ENVIRONMENTAL TREATIES
DECREASE FRAUD AND MANIPULATION

ENERGY
INCREASE EFFICIENCY WITH P2P ELECTRICAL GRIDS
IMPROVE ACCESS TO POWER IN AREAS WITH POVERTY OR NATURAL DISASTERS

NON-PROFITS
TRACK WHERE DONATIONS ARE GOING
DECREASE INEFFICIENCY AND BUREAUCRACY IN CHARITIES

RECYCLING
ENCOURAGE RECYCLING BY PROVIDING TOKENIZED REWARD
TRACK AND EVALUATE EFFICACY OF RECYCLING PROGRAMS

CARBON TAX
CALCULATE TAX FOR PRODUCTS BASED ON CARBON FOOTPRINT
CREATE A REPUTATION SYSTEM FOR COMPANIES BASED ON EMISSIONS

SUPPLY CHAINS
TRANSPARENTLY TRACK PRODUCTS FROM ORIGIN TO STORE SHELF
REDUCE CARBON FOOTPRINT AND UNSUSTAINABLE PRACTICES

CHANGING INCENTIVES
ALIGN INCENTIVES WITH SUSTAINABLE PRACTICES
CREATE INCENTIVES FOR PEOPLE TO ACT IN SUSTAINABLE WAYS

CREATED BY FUTURETHINKERS.ORG

INFORMATION BY BCDC.ONLINE

The blockchain can be used to transparently track a variety of data like the carbon footprint of each product, the greenhouse gas or waste emissions of a factory, or a company's overall history of compliance to environmental standards.

Does blockchain have environmental impact?

Blockchain technology is a decentralized and distributed digital ledger maintained by a computer network. Blockchain technology has a significant carbon footprint due to its energy-intensive process of verifying transactions and creating new blocks on the blockchain.