THE FUTURE APPLICATION OF BLOCKCHAIN TECHNOLOGY

SATRIA YUDISTIRA IRAWAN

Abstract. The introduction of Bitcoin has made the idea of blockchain become popular. Blockchain technology has data that is immutable, making it very secure, and transparent because every record of all the contents of the transaction data can be known from one server to another server. The implementation of blockchain can be much bigger than now it is today. This paper will present an overview of blockchain technology, how the blockchain network works, and the future application of blockchain.

1. Introduction

Blockchain adoption is almost like the adoption of the internet in the 1990s. During that time, only a few people use the internet so accomplishing anything was difficult, and searching for some information is challenging (Quartz). The same things applied to blockchain nowadays; only some institutions have already implemented this technology. The CEO of JP Morgan, Jamie Dimon shares his thought about blockchain and it is future during the annual letter to shareholders saying that "Decentralized finance and blockchain are real, new technologies that can be deployed in both public and private fashion, permission or not". Furthermore, he further states that "We believe there are many uses where a blockchain can replace or improve contracts, data ownership, and other enhancements"(Helms).

Not only did Jamie Dimon think positively about blockchain; the richest man on earth Elon Musk also shares his thought on blockchain technology, specifically Bitcoin. According to Forbes, Tesla CEO Elon Musk on the future of Bitcoin and crypto states that "Musk was then asked to share how he felt after he read Satoshi Nakamoto's Bitcoin white paper for the first time, to which the Tesla CEO responded, "I thought it was pretty clever." and also Musk also states that "Where I see crypto as is effectively a replacement for cash," said Musk. "But not as a replacement for a primary — I do not see crypto being the primary database" (Torpey). Some influential person has shown positive thought toward blockchain technology. It is important for us to learn about blockchain technology because sooner or later, I believe there will be more and more influential people starting to implement this technology in their companies.

The emergence of blockchain technology can change the current centralized systems, and improve security and integrity. It is very difficult to attack the systems due to it being Proof-of-Work, this resulting attacker having a very powerful computing power. Quoting, Sana Alfreen from Simplilearn states that "Blockchain helps in the verification and traceability of multistep transactions needing verification and traceability. It can provide secure transactions, reduce compliance costs, and speed up data transfer processing. Blockchain technology can help contract

management and audit the origin of a product" (Alfreen). Not only blockchain are secure, it is also transparent making it traceable resulting in lesser fraud in the systems.

Perhaps having a greater understanding of blockchain technology will advance globalization and our systems. To quote, Charles Darwin said that "It is not the strongest or the most intelligent who will survive but those who can best manage change" (Darwin). Adapting to new things will be challenging, but do not expect greater results if we still doing the same things. This paper will show what blockchain technology is and how blockchain technology is one of the best ways to enrich an individual's life.

2. History of Blockchain

The blockchain's emergence is far beyond the invention of Bitcoin (2008) and even before the dot-com bubble (the 2000s). Interestingly, the invention of Bitcoin made this idea about blockchain emerge and reach popularity and gain more and more people's attention. According to Gwyneth Iredale from 101Blockchains, she states that "Stuart Haber and W. Scott Stornetta envisioned what many people have come to know as blockchain, in 1991. Their first work involved working on a cryptographically secured chain of blocks whereby no one could tamper with the timestamps of documents. In 1992, they upgraded their system to incorporate Merkle trees that enhanced efficiency thereby enabling the collection of more documents on a single block" (Iredale). At that time, people are not interested in digging deeper into this invention and cannot convince enough people to use this invention.

During the 2008 financial crisis, some people distrusted the financial institution and the government regulation. According to Shaikh Saleem from Mint, he states that "When iconic US investment bank Lehman Brothers Holdings Inc. filed for bankruptcy in 2008, it shook people's faith in banks so much that a new class of asset, which did not have the backing of any formal bank, came into being. Bitcoin, the most popular cryptocurrency, was first found mentioned in November 2008, about two months after the Lehman crisis" (Saleem). The relying on the centralized bank might have caused the crisis in 2008. The emergence of Bitcoin is when people realized there was a flaw in the central systems.

After the crisis, the pseudo-anonymous person or group called Satoshi Nakamoto created the digital currency that removes the intervention of third parties. They then publish the white paper called "A Peer-to-Peer Electronic Cash Systems" and according to Bitcoin White paper, they wrote that "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" (Satoshi 1). This is the beginning of the idea of blockchain gaining popularity and making some people interested to use this idea and decentralized systems on other sector.

3. Mechanism of Blockchain Technology

The mechanisms of blockchain to create trust between party was essential. Before the use of blockchain technology, the trust between parties was delivered through a trusted third party. Without intermediaries, the blockchain network elements are:

- Ledger: The record of full transactional history. The transaction and values in the blockchain ledger are not overridden. The chaining in the blockchain

ensures that the data in the ledger has not been tampered with and the data is attestable (Yaga 2).

- Shared: The blockchains are secure and also transparent because the ledger is shared amongst multiple node participants in the network. Blockchain technology is a form of distributed ledger meaning that the number of nodes in a network can be increased to make it more resistant to attacks. If the number of nodes increases, attackers will have difficulty sabotaging the systems due to the increase in the consensus protocol. Although it is shared, blockchain technology has two categorizations; a permissioned blockchain network is like a corporate, where only selected participants can participate, while a permissionless blockchain network is like the public internet, where anyone can participate (Yaga 2).

These are the important keys to ensuring the blockchain is trusted and secured. The cryptographical security of the blockchain is because of the technology working behind the scenes. To understand more about blockchain technology, it is important to know about the blockchain pieces:

- Cryptographic Hash Functions: is the process that calculates a unique output based on an input of any size. The output will be displayed as 64 character hexadecimal string with a size of 32 bytes, called a digest. If the smallest change from the input occurs then the output will be different, the purpose of hashing is to prove that the data has not been altered. In blockchain technology, some of them use the SHA256 hashing method (Yaga 7).

- SHA-256: it is stands for "Secure Hash Algorithm 256-bit." The SHA-256 is used to hash a message that has a length of k bits where $0 \leq k \leq 2^{64}$. The SHA-256 algorithm use 1) a message schedule of sixty-four 32-bit words, 2) eight working variables of 32 bits each, and 3) a hash value of eight 32-bit words. After performing the computation, the final result of SHA-256 is a 256-bit message digest (Dang 21). Since this paper is not focusing on the SHA-256, additional information on how to do the computation can be further read in the FIPS PUB 180-4 document.

- Asymmetric-Key Cryptography: cryptography system where the user has a private key and is used to generate the public key. Users can digitally sign data with the private key and verified using the public key. The purpose of the Asymmetric-Key Cryptography is to verify that the user transferring value to other users is the rightful owner and can prove it by signing the transaction. It is something similar to the signing process of a document, but in this case, the signature will be the owner's private key. This process is the safest way to the signature because it is hard to be fake. The private key will be kept secret and the public key is made public as an address. In blockchain technology, the private key is used as a digital signature and store wallet; the public key will be used to derive the address (Yaga 11).

- Digital Signature: a cryptographic technique that uses the asymmetric key to determine authenticity, reputation, and integrity. Some blockchain technology uses ECDSA Algorithm (Yaga 11). The private key is used for a period of time and the public key can be used as long as the digital signatures that have been generated using the associated private key need to be verified. The ECDSA digital signature shall be generated using 1) Domain parameters that have been generated, 2) A private key that has been generated, 3) A per-message secret number that has been generated, 4) An approved has function and lastly, 5) An approved random bit-generator (Barker 26). To have a deeper understanding of ECDSA, read the FIPS PUB 186-4 document.

- Wallet Address: The address is derived from the user's public key using a cryptographic hash function. The purpose of the address is similar to the usage of routing numbers and account numbers in modern banking. The transaction will visible only as of the user address and receiver (Yaga 12). In blockchain technology, the Wallet address looks as follows: "32xMvWc1dz89dTkzqUFwG1h9diBZK5pasf" it is an alphanumeric string.

- Private Key Storage: the private key is a variable in cryptography with the purpose to encrypt and decrypt data. It is typically a long, randomly generated sequence of bits that are hard to guess. The private key is very important to keep secret and only the rightful owner has to access to it. Some people use software to securely store them, and the software is also known as a Wallet. The Wallet contains public keys, private keys, addresses, and also the data or the digital asset the user has. If the private key is lost or stolen the digital asset and the data will also be stolen or lost because if the attacker has the private key, they have full access to the wallet. The private key storage is performed like a digital safe box (Yaga 13).

- Node: Individual system within the blockchain network. The purpose is to publish a new block as well as verified the transaction is valid. The publishing node is the one that publishes a new block to the network (Yaga 3).

- Smart Contracts: Yaga share his thought on Smart contract, he stated that "A collection of code and data that is deployed using cryptographically signed transactions on the blockchain network. The smart contract is executed by nodes within the blockchain network; all nodes must derive the same results for the execution, and the results of execution are recorded on the blockchain." The document further writes that "A smart contract can perform calculations, store information, expose properties to reflect a publicly exposed state and, if appropriate, automatically send funds to other accounts" (Yaga 32). To understand more about smart Contracts in blockchain read the NISTIR 8202 document page 32.

Blockchain technology stores the transactions and data in a block that is attached to another block. This will be resulting in a chaining block, and this is why it is called Blockchain. The blockchain's block structure is as follows (Yaga 15):

- Genesis Block: the first block in the blockchain network, records the initial state of the blockchain systems.

- Block: Transaction that has been added to the blockchain by the publishing node will be published to the blockchain network as the block. The block will contain the block header and block data. The block header and block data will contain as follows :

  (1) Block Header:
      (a) The block number or block heights.
      (b) Previous blocks header's hash value.
      (c) Hash of representation of the block data (usually contains the hash of the Merkle root (Merkle root is the hash of all the hashes value of all the transactions in a block).
      (d) Timestamp.
      (e) The size of the block.
      (f) The nonce (arbitrary number that is used once to solve a hash puzzle).
  (2) Block Data:
      (a) List of validated transactions within the block.
      (b) Other data.

4. Consensus Protocol

What makes blockchain secure is because of the network and systems. Mike Orcutt from MIT Technology Review, believes that blockchain is secured because of "a cryptographic fingerprint unique to each block, and a "consensus protocol," The process by which the nodes in the network agree on a shared history" (Orcutt). The blocks in the blockchain are cryptographically secured and also the consensus protocol makes the blockchain technology tamper-proof. This consensus protocol have a very important role in blockchain technology. There are a lot of consensus models that some blockchain technology use such as Proof-of-Stake, Round-Robin, Proof-of-Authority, and lastly, Proof of Elapsed Time. To learn about each model, read NISTIR 8202 document section 4. In this paper, we gonna show how the first consensus model in the blockchain works.

4.1. **Proof-of-Work.**

To understand how the proof-of-work works, the concept of blockchain mining needs to be fluent. In the blockchain ecosystems, every block is created and validated by the miners. Miners is a system or node that participates in the blockchain transaction, in turn, plays a crucial role both in creating new blocks and in verifying transactions on the blockchain. It will add new blocks to the existing chaining blocks and ensures that only valid transaction and block are added to the blockchain. To publish a new block to the blockchain, miners need to do a mining process.

The mining process needs to solve a computationally intensive puzzle, this is where the proof-of-work consensus is born. The solution to the puzzle is the "proof" that they have performed the work. Further, Proof-of-Work is a consensus model where a publishing node wins the right to publish the next block by expending time, energy, and computational cycles to solve a hard-to-solve, but an easy-to-verify problem. According to blockchain expert Henrique Centieiro "The mathematical problem is nothing more than guessing a nonce, a long string of numbers with millions or billions of trial and error. In order words, brute-forcing the result. A miner must guess a nonce, add it to the hash of the current header, rehash the value, and compare the result to the target hash" (Centieiro). The difficulty of the mining process is represented by how hard it is to find the hash needed, the miners need to guess the number of possibilities or combinations of the hash, and the more miners try to find the hash, the more difficult and longer it needs to solve the problem. If the miners successfully perform the proof-of-work they will receive the Block reward as the reward for their intensive work.

Interestingly, if the miners have more hashing power and a higher hash rate(the rate the processor can calculate for the cryptographic hash function); the miners with lower hashing power and lower hash rate will still be able to compete with each other because there are lottery system mixed in the process. For easier to understand, imagine the miner wants to mine gold in the gold mine; then the miner needs better equipped to compete with other miners. Although the miner has better equipment and can dig faster than others, does not mean the miner will always get the gold because in the process there will be a lucky spot that has gold in it. The decentralized systems make the distribution of the network away from the central group or systems. Moreover, The decentralized systems make all nodes in the blockchain network participate in the validation process. So, the more node participates in the network the more secure it will be, because each member node must validate all data being added to the network. Thus making it safer but also making it slower. This makes the blockchain network very unlikely to be attacked because the attacker needs to have very massive computing power in order to alter the block in the network without being noticed by another node and if the attacker has such massive power, they will rethink again to do it because it is better for them to participate in the network to get the block rewards from the proof-of-work model.

5. Bitcoin Network

Bitcoin is the first digital currency that utilizes blockchain technology to prevent double-spending. Unlike paper money, Bitcoin is a cryptocurrency, which means it does not have a physical form, it looks like lines of codes (Yurina). Proof-of-Work consensus model plays a huge role in the Bitcoin ecosystem, the miners in the Bitcoin verify the transaction and create new blocks for the network. All the valid transactions but unconfirmed have to enter a waiting area before they are accepted in a block. This waiting area is known as the Mempool (Sen). The transaction that is accepted in a block will be confirmed, and the time needed for the transaction to be confirmed is around 10 minutes. The miners need to solve a computationally intensive puzzle to find the nonce of the next block. Interestingly, Bitcoin's software adjusts the difficulty miners need to solve. Hence, every block of transactions is created approximately every 10 minutes. Each block will have

a limit of 1 MB of transactions. Thus, the volume of transactions is digestible (Floyd). The Bitcoin mining difficulty is adjusted every 2,016 blocks mined added to the network(approximately every two weeks), and the difficulty is increased or decreased by the leading zero of the nonce.

Miners are rewarded with Bitcoin as a block reward and transaction fees for successfully creating the block. The Bitcoin digital currency can only be obtained through the block reward. Moreover, this reward is cut in half every 210,000 blocks mined, approximately every four years. This event is called the halving. The system is built-in as a deflationary one for the rate at which new Bitcoin is released into circulation (Floyd). The maximum circulating supply of Bitcoin is 21 million, if the amount of Bitcoin reaches the maximum, the miners will only be rewarded with the transaction fees. After the miners successfully published the block into the network, other nodes will verify the block, and the update is distributed across the network. Consequently, each node in the network will have a copy of the block.

6. Blockchain Transaction

The most important about blockchain is it's transaction, the transaction is which makes the blockchain the future of the record-keeping and the financial systems. The blockchain transaction works as follows. Let's assume that person A wants to make a transaction with person B. In this scenario, Proof-of-Work is used in the blockchain network, the process will be as follow: (Yaga 9)

(1) A sends the transaction to B using B's Wallet address.
(2) The transaction is received with the information about the sender, receiver, and the transaction.
(3) The transaction is signed by A's digital signature with A's private key to show that A's authorized the transaction. After that, the transaction is broadcasted into all nodes that have a copy of the blockchain. The purpose of each node is to verify that the transaction is legit and the digital signature is valid, the miners use A's public key to verify this. The transaction right now is still in the unconfirmed transaction because it waiting for the miners to create the blocks to be mined by finding the nonce values.
(4) The miners will do the proof of work to solve the math puzzle. If the miner solves the block, the block will then add into the blockchain network and the transaction will be confirmed.
(5) The miners will receive the reward, and other nodes will verify the result and spread the copy of the block to other nodes
(6) The transaction is recorded into the blockchain and B receives the transaction.

6.1. **Chaining Blocks.**

The transaction in the blockchain is stored in the form of blocks, every block is chained together to another block, thus forming the blockchain. If the previous block is altered, it will have a different hash. Due to, all subsequent block to have different hashes. The creation of a block header hash consists of a timestamp, the previous block header's hash values, the nonce, the hash of the block data, and the size of the block. The hashing process uses the Merkle Root which hashed transaction hashes within the transaction. Meaning

that each hashed is further hashed with the timestamp included, the process will hash the data and combined it until there is a singular root hash that represents the whole structure of the block (Satoshi 5). This in turn, would cause all subsequent blocks to also have different hashes since they include the hash of the previous block. Makes it possible to easily detect and reject altered blocks. To help better understand this process, below is an example of how the chaining blocks together works (this is not from an actual blockchain network).

(1) Block(1):
Time creation: 2022-05-07 18:33:20
Blockchain data: Genesis Block
Previous Hash: 0
Block Hash: da1a7b7fdcb5e5c782ef131b31a1bff9d893f75484b8dbbdaa53ea1624c277

(2) Block(2):
Time creation: 2022-05-07 18:33:24
Blockchain data: Block 1
Previous Hash: da1a7b7fdcb5e5c782ef131b31a1bff9d893f75484b8dbbdaa53ea1624c277
Block Hash: b6d43618b042c88ebfcfd84eadc68f35b34e6fe8d85d6cc8ff9038fdc6671e3e

(3) Block(3):
Time creation: 2022-05-07 18:33:37
Blockchain data: Block 2
Previous Hash: b6d43618b042c88ebfcfd84eadc68f35b34e6fe8d85d6cc8ff9038fdc6671e3e
Block Hash: ca60f2ac5bab246c071a935806c4006912e6f397a6eb052ae9aba5fd0d65

(4) Block(4):
Time creation: 2022-05-07 18:33:43
Blockchain data: Block 3
Previous Hash: ca60f2ac5bab246c071a935806c4006912e6f397a6eb052ae9aba5fd0d65
Block Hash: 69f0292d4513688e0113149b097e8a7f3902fb8608ef5ab9173fb16a81577

As we can see the Block will consist of the block hash and the previous hash and form chaining blocks. The block hash obtained from hashing the timestamp, previous block hash and block data. If we altered the block, the block hash and the previous hash will be changed thus the blockchain will no longer be valid. Let's assume we altered the blockchain, by deleting one of the blocks; in this case, block data "Block 1".

(1) Block(1):
Time creation: 2022-05-07 18:33:20
Blockchain data: Genesis Block
Previous Hash: 0
Block Hash: da1a7b7fdcb5e5c782ef131b31a1bff9d893f75484b8dbbdaa53ea1624c277

(2) Block(2):
Time creation: 2022-05-07 18:33:37
Blockchain data: Block 2
Previous Hash: b6d43618b042c88ebfcfd84eadc68f35b34e6fe8d85d6cc8ff9038fdc6671e3e

Block Hash: ca60f2ac5bab246c071a935806c4006912e6f397a6eb052ae9aba5fd0d65

(3) Block(3):
Time creation: 2022-05-07 18:33:43
Blockchain data: Block 3
Previous Hash: ca60f2ac5bab246c071a935806c4006912e6f397a6eb052ae9aba5fd0d65
Block Hash: 69f0292d4513688e0113149b097e8a7f3902fb8608ef5ab9173fb16a81577

(4) Block(4):
Time creation: 2022-05-07 18:34:10
Blockchain data: Block 4
Previous Hash: 69f0292d4513688e0113149b097e8a7f3902fb8608ef5ab9173fb16a81577
Block Hash: 3952c460a18a8471256815e2e553443543b15749ecddf726db768303d7e5e6

Since Block 1 has been deleted, the chain will no longer be valid because the Block 2 previous hash will not match it is the previous block hash, thus the blockchain will not be valid. Let's take a look at the figure below.

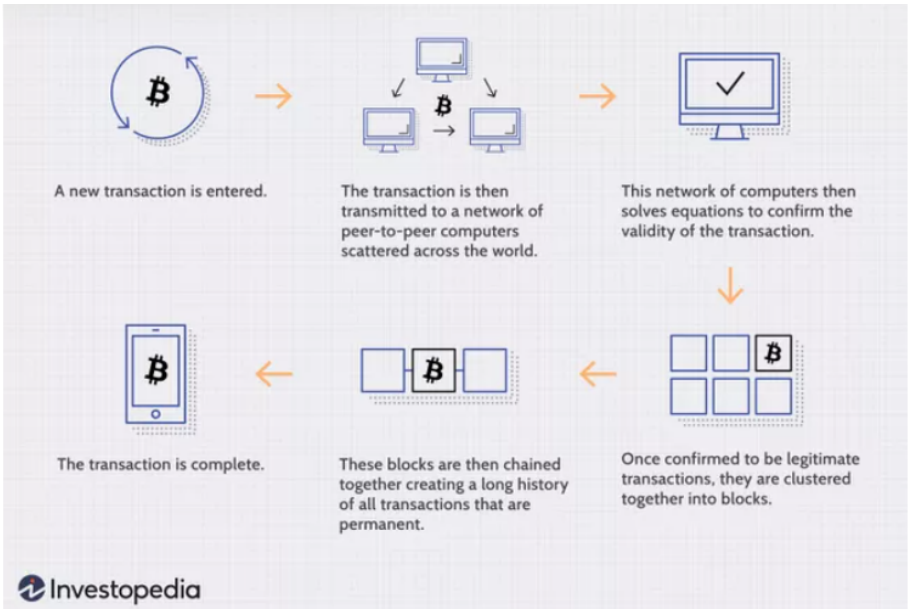

FIGURE 1. Image of the blockchain transaction `Blockchain Transaction`

Figure 1. shows how the transaction is recorded in the blockchain according to Investopedia. The transaction/record is secured in the blockchain through cryptography. The Network participants have their own private keys(in the above case is A's private key) and are assigned to the transaction they made and also for digital signature purposes. If the transaction is altered, the digital signature will invalidate and the network will be invalid because it has been altered and the network will know that there is damage in the network. The secure thing about blockchain is its decentralized network, so the attacker will have a hard time to attack the networks because it is distributed across the networks and continually updated and kept in sync.

Blockchain networks are distributed across the network, and do not have a central node. Therefore, no single point of failure and cannot be changed from a single computer. The way to alter the networks is to have the computing power to access every instance in the network for at least 51 percent majority, and alter all at the same time. That is why the more people use the blockchain or the bigger the network is, the more secure the blockchain will be. The attacker will need a very powerful computing power that can cause so much money to be able to alter the blockchain network.

7. Application of Blockchain Technology

Blockchain technology can be used for many things. The first application of blockchain technology was used for Bitcoin, as a cryptocurrency. Cryptocurrency is one of the many other applications that can be used by blockchain technology, it can be used for supply chain problems, proof of ownership, and also proof of authenticity of an item. For instance, digital artworks that are embedded into the blockchain. Gladstone from WNYC Studio stated that "Anil Dash and Kevin McCoy first invented what we know today as the NFT, or non-fungible token, to empower artists to sell digital works. (In case you missed it: NFTs are unique units of data that can be linked to media such as videos or images)" (Gladstone). Since blockchain is immutable, it is easy to be used to proof of authenticity. That is why in the arts it is very important to proof of ownership and authenticity, because digital arts can easily be fake and it is hard to prove that it was the genuine ones.

With blockchain, it removes the third party, in this case, the experts that verify the arts, because blockchain has all the block data so it can be traced to its originality. Quoting, Alex Nelson from the National World, states that "Forgeries are difficult when replicating physical art, thanks to the cumulative expertise of art historians and experts around the world, and the technology that can be used to rat out fakes. But when dealing with digital art, pieces can be copied much more readily, usually with just the simple duplication of a file. NFTs put an end to that, encrypting the digital source of artwork with blockchain to ensure it remains the definitive version of that piece" (Nelson). Although the digital arts can be copied multiple times, the blockchain technology can verify the real owner of that original digital art.

Some people might not be interested in the NFT because it does not affect everyday life. However, blockchain is more than that. Whether people realize it or not, blockchain can improve supply chain issues and many industries. The supply

chain plays a huge role in items' price if the supply chain has some issues or is even stuck the price of goods will be increasing that is why having a good supply chain is necessary to maintain the stability of goods prices. Walmart is one of the biggest retail companies in the world. Although Walmart is a big company, it still has some issues. Kate Vitasek and the team from Harvard Business Review wrote that "Walmart has long been known as a leader in supply chain management. However, its prowess could not insulate it from a problem plaguing the transportation industry for decades: vast data discrepancies in the invoice and payment process for freight carriers, which required costly reconciliation efforts and caused long payment delays" (Vitasek).

The logistics of the massive quantities of goods across the countries with different time zones, climates, and borders have some operational challenges. Imagine, each load shipped requires tracking data points and temperature updates that need to be calculated and incorporated into each invoice. With such massive data points that needed to be factored into invoices, the invoice and payment process could be fraught with data discrepancies. With 70% of invoices requiring reconciliation efforts, it increased transaction costs and unhappy carriers waiting for payments (Vitasek).

The main problem with this is because the use of multiple information systems between Walmart Canada and it is carriers that could not talk to each other. Therefore, reconciliation had to be performed manually which cause a labor-intensive, time-consuming process riddled with inconsistencies - according to Harvard Business reviews. To solve these issues, according to that article, Walmart Canada works together with DLT Labs, a leader in developing and deploying innovative enterprise solutions using distributed ledger technology. The systems(called DL Freight) continuously gather information at every step, from the tender offer from the carrier to the proof of delivery and the approval payment (Vitasek).

This process is automatically captured and synchronized in real-time and only visible to the parties involved in the transaction. According to that article, the result was "Prior to DL Freight over 70% of invoices were disputed. Today less than 1% of invoices have discrepancies, and these disputes are easily flagged and quickly resolved. Gone are the days of payments taking weeks or months; carriers are now getting paid on time" (Vitasek). With the help of blockchain, Walmart Canada can solve it is supply chain issues. Because Blockchain is a decentralized network, meaning that the systems rather than relying on a single system, communicating with all the network systems thus the systems can talk with Walmart Canada and it is carriers, and the reconciliation can perform automatically.

The future of blockchain technology is limitless, perhaps it can be used in many sectors such as entertainment, banking, government, education, healthcare, and many more. According to CBInsight, there are 65 big industries blockchain can transform. Some of them are, Wills and Inheritance; the blockchain technology will help identify the factual information, provide verifiable transaction data, and dismiss claims that are without merit. In automotive manufacturing, blockchain technology can track its ownership and store information about the car's status.

In Education, blockchain could verify the educational credits and education record thereby reducing fraudulent claims of unearned educational credits and altered transcripts ("65 Big Industries Blockchain Could Transform"). To sum up,

according to the CBInsight article the sectors that could improve by blockchain technology are Financial Services, Travel, and mobility, Infrastructure and energy, Healthcare, Government, Retail and CPG(Consumer Packaged Goods), Agriculture and natural resources, Information and communication, Entertainment, and Enterprise tech. The application of blockchain in cryptocurrency is the first step on the other bigger steps for other crucial things ("65 Big Industries Blockchain Could Transform").

In the early invention of blockchain, Bitcoin has been used as a currency for some people to buy illegal items and used for money laundering. The stain of the Bitcoin in its early days is not because of the technology, but passiveness of the government and society's to regulate and use this technology to their own society. Nowadays, some people have already tried to implement and use blockchain technology to solve everyday problems and make the world more convenient and secure. Perhaps most of all, a deeper understanding of blockchain technology can lead to greater cybersecurity and quality of life and transform the world into a better world.

References

[1] Afreen, Sana. "Why Is Blockchain Important and Why Does It Matters." *Simplilearn.com*, Simplilearn, 16 Feb. 2022, https://www.simplilearn.com/tutorials/blockchain-tutorial/why-is-blockchain-important#:~:text=Blockchain%20helps%20in%20the%20verification,the%20origin%20of%20a%20product.

[2] Barker, E. (2013), Digital Signature Standard (DSS), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.186-4

[3] CB Insights. "65 Big Industries Blockchain Could Transform." *CB Insights Research*, CB Insights, 28 Mar. 2022, https://www.cbinsights.com/research/industries-disrupted-blockchain/.

[4] Centieiro, Henrique. "Bitcoin Proof of Work-the Only Article You Will Ever Have to Read." Medium, Level Up Coding, 20 May 2021, https://levelup.gitconnected.com/bitcoin-proof-of-work-the-only-article-you-will-ever-have-to-read-4a1fcd76a294.

[5] Dang, Q. (2012), Secure Hash Standard (SHS), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.180-4

[6] Floyd, David. "How Bitcoin Works." Investopedia, Investopedia, 2 May 2022, https://www.investopedia.com/news/how-bitcoin-works/#toc-how-does-bitcoin-work.

[7] Gladstone, Brooke. "A Tech Pioneer Reckons with the NFT Craze He Helped Create: On the Media." *WNYC Studios*, 12 Nov. 2021, https://www.wnycstudios.org/podcasts/otm/segments/nft-inventor-reckons-industry-he-created-on-the-media.

[8] Iredale, Gwyneth. "History of Blockchain Technology: A Detailed Guide." *101 Blockchains*, 21 Dec. 2020, https://101blockchains.com/history-of-blockchain-timeline/.

[9] Kevin Helms, et al. "JPMorgan CEO Jamie Dimon to Shareholders: Decentralized Finance, Blockchain Are Real – Featured Bitcoin News." *Bitcoin News*, 8 Apr. 2022, https://news.bitcoin.com/jpmorgan-ceo-jamie-dimon-to-shareholders-decentralized-finance-blockchain-are-real/.

[10] Murphy, Mike. "From Dial-up to 5G: A Complete Guide to Logging on to the Internet." *Quartz*, Quartz, https://qz.com/1705375/a-complete-guide-to-the-evolution-of-the-internet/.

[11] Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

[12] Nelson, Alex. "What Are Non-Fungible Tokens? the Crypto Technology Taking over the Digital Art World." *NationalWorld*, NationalWorld, 25 Feb. 2022, https://www.nationalworld.com/lifestyle/money/nft-meaning-crypto-art-tech-explained-what-is-a-non-fungible-token-where-to-buy-them-and-best-marketplace-3163733.

[13] Orcutt, Mike. "How Secure Is Blockchain Really?" *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/.

- [14] Saleem, Shaikh Zoaib. "The 2008 Global Meltdown and the Birth of Bitcoin." *Mint*, 13 Sept. 2018, https://www.livemint.com/Money/YTYMYUD7dytGK5PGSpdRTN/The-2008-global-meltdown-and-the-birth-of-Bitcoin.html.
- [15] Sen, Sahil. "How to Access Bitcoin Mempool." QuickNode, 12 Apr. 2022, https://www.quicknode.com/guides/defi/how-to-access-bitcoin-mempool.
- [16] Torpey, Kyle. "Tesla CEO Elon Musk on the Future of Bitcoin and Crypto." *Forbes*, Forbes Magazine, 23 Jan. 2020, https://www.forbes.com/sites/ktorpey/2020/01/23/tesla-ceo-elon-musk-on-the-future-of-bitcoin-and-crypto/?sh=18f4ae4c7500.
- [17] Vitasek, Kate. "How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenges." *Harvard Business Review*, 5 Jan. 2022, https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges#: :text=Then%20Walmart%20Canada%20pioneered%20a,70%20third%2Dparty%20freight%20carriers.
- [18] Yurina, Vera. "What Does a Bitcoin Look like? A Detailed Insight into the Technology and Currency." U.Today, 15 Dec. 2019, https://u.today/guides/blockchain/what-does-a-bitcoin-look-like-a-detailed-insight-into-the-technology-and-currency.
- [19] Yaga, Dylan. Blockchain Technology Overview - NIST. 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.