The Distributed Ledger Technologies in Agriculture (DLT)

Chapter 3: Distributed Ledger Technologies in Agriculture

Introduction

In the early times, people used to buy and sell by barter and then by currency. The selling process was done as soon as the goods were delivered, and the agreed payment was received. However, when people started to sell in installments or deferred payment, they needed to log data for each sale: its total price, the down payment, the number of installments, and the next payment's due date. All of this information was logged in a notebook called the ledger. The only problem with the ledger is that its owner can alter it. Thus its information does not necessarily reflect reality. Ledger alterations include adding false sales, modifying the prices of the payments, and canceling or omitting a transaction. To solve this problem, the duplicate ledger idea appeared. In this concept, each party, the buyer and the seller has a ledger copy. Thus any transaction should be written in the two ledgers and signed by both parties to be validated. However, the accuracy of transactions will not be guaranteed, especially with frauds in either party. Still, if the two copies of the ledger differ, who is considered correct?

On the other hand, purchasing high-priced entities such as houses and lands needed more than just logging the sales process between the seller and the buyer. They used to register the sale through a third party, often a governmental organization or a trusted individual. The third-party influence causes many problems, including the costs or fees of registration, the time it takes, and the regulations it might impose on the seller and the buyer. Still, the third party does not guarantee the security of the records, as they might be stolen or damaged.

Digitizing the logging processes solved some of the problems, as the process is easier and faster to log and retrieve. However, security and third-party problems still exist; the digital ledgers can also be altered by hackers and can be lost by any hardware failure. Hence, we need a method to keep our ledgers secure, immutable, auditable (easy to access), and decentralized (no third party). These goals are all achieved in one technology, which is distributed ledger technology.

The distributed ledger technology

The distributed ledger technology (DLT) started in 1991 when Haber and Stornetta introduced a method to timestamp a digital document (184) through hashing the contents. Hashing is a type of irreversible encryption. Encryption is a method that converts readable text to an equivalent text that is unreadable (in most cases) to protect the original text from being exposed by unauthorized persons while moving or storing it. The encrypted text can be restored by decryption, which follows a reversed path to retrieve the original text. The method that encrypts and decrypts the text uses a so-called key known only by the authorized personnel.

Encryption versus hashing

To understand the difference between encryption and hashing, we can take the following example. We know in the ASCII code of letters (185,186), the uppercase letters A to Z took the values of 65 to 90, while the lowercase letters a-z took the values 97 to 122. If we have the word “UN”, it has two uppercase letters, “U” and “N” , with values 85 and 78, respectively. One of the encryption methods is to join the ASCII codes of the letters to be 8578. So, when the authorized person receives the code, he

knows how to reverse the operation, as he has the "key" of the decryption by splitting the numbers, then use the ASCII table to know which letters represent these codes.

On the other hand, if we want to hash the text, we apply a formula that generates a code; this code is fixed every time we apply the formula to the exact text. For example, we can hash the same word by adding the two numbers 85+78=163. Hence, we send the original document combined with its hashing value. The receiver knows the hashing formula, he applies it to the received text and compares the resulting hash to the original hash. If they match, then this guarantees that the document has not been altered.

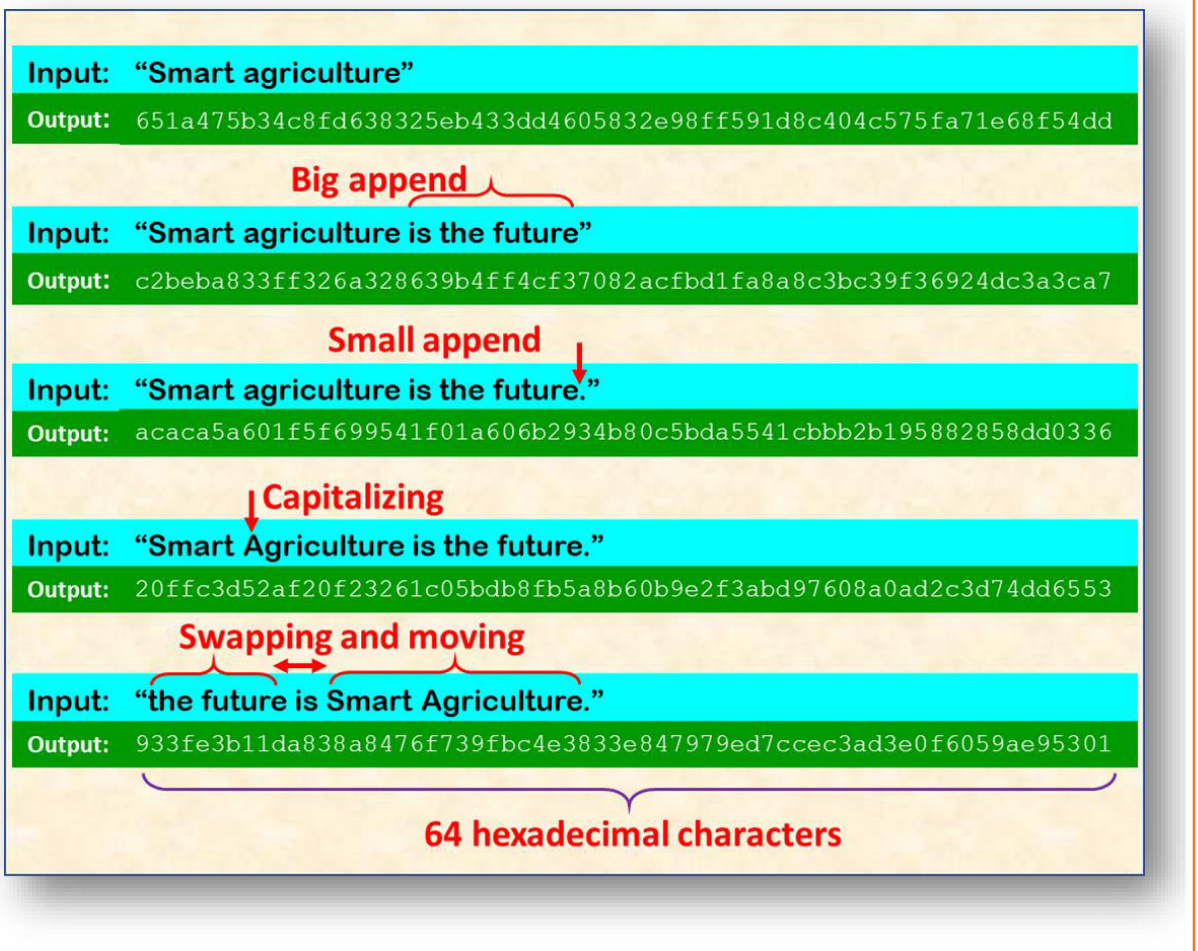

Figure 18. The change in the SHA256 output hash as affected by the change in input.

If you notice, no one can predict precisely the original text from its hash value, even if he knows the hashing algorithm and the hashing value, because the hash value can result from infinite numbers of letters combinations. For example, we know the 163 is the hashing value, but we do not know the number of letters of the original text. However, if we knew that it is of two letters, they can be any two letters having the sum of their ASCII code is 163, including "MV", "Ab", and even "NU" (the reverse of UN).

This example shows the difference between encryption and hashing. Of course, the encryption and hashing algorithms shown here are too simple, and the actual algorithms are much more complex.

The SHA-256 hashing algorithm

As we said, the hashing algorithms are way more complex than the example we showed. In 1991, the National Security Agency (NSA) of the United States published a secure hash algorithm (SHA) with different bits ranging from 224 bits to 512 bits. The most common algorithm is the SHA-256 algorithm which has different implementations and applications in monetary and security fields. The main properties of this algorithm are as follows:

- The hash length is always 256 bits in length, regardless of the length of the input string, i.e., if the input is one character, the output will be 256 bits in length, and if the input is a billion characters, the output will also be 256 bits length. In the hexadecimal system, we can represent every 4 bits as one character. Thus the output of the SHA-256 is usually represented in hexadecimal format as 64 characters.
- Any change in the original text leads to a dramatic change in the resulting hash value. Even a single period in a million-character text can change the hash entirely if added, moved, or removed, as shown in Figure 1. The figure shows that the SHA output of each text is entirely different from each other, regardless of whether the change is small or big, by changing the case of even one letter or even swapping the exact words of the sentence. Each of which leads to a new hash value that has no link to the old one.
- It is important to mention that it is impossible to predict the change in the hash value regarding any change in the original text, the only way to see the change is to try hashing each new text to see the reflection on the hash.

The data block

In 2002, Mazi`eres and Shasha (187) introduced a new file system that stores data in a group of blocks. Each block is secured using a hashing algorithm that depends on the previous linked block and is replicated throughout the network members. The data block, Figure 3, is constructed of two main components: the header and the transactions list. The header includes the timestamp where the block was created, the hash value of the previous block in the network, the nonce (will be described), and other technical data, including the hashing protocol used, the difficulty level, and other metadata. The transaction list includes each transaction amount and direction, from whom to whom, the balance of the sending party before and after the transaction, combined with the proof that each party approves the transaction by public and private keys.

To close each block and ensure that its contents are secured and immutable, a unique hashing is performed to the entire contents of the block, including a random number used to reach the target hashing condition. This random number is called the number that is used only once, or the Nonce.

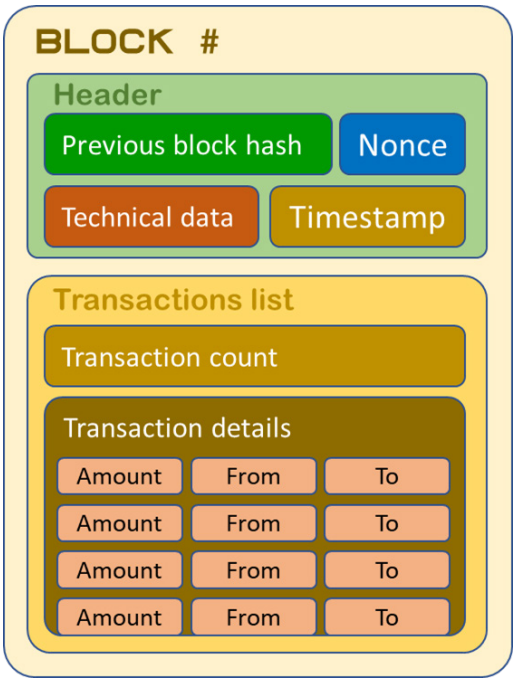

Figure 20. An illustration of a data block.

As we said, the hash consists of 64 hexadecimal digits. If we take our example in Figure 1, the last hash starts with `933f`. What if we want the hash to start with a zero? It is not possible unless we change the input text by adding some digits or characters. Thus, we add a random number to the original text, then test the change to the hash. If the first digit of the hash becomes zero, then the Nonce is added to the block, and the block is considered closed. Otherwise, we will try another Nonce and check. This operation is repeated until we reach our target. For example, if the target is four zeros at the beginning of the hash, then the Nonce should be 79532, as shown in Figure 2.

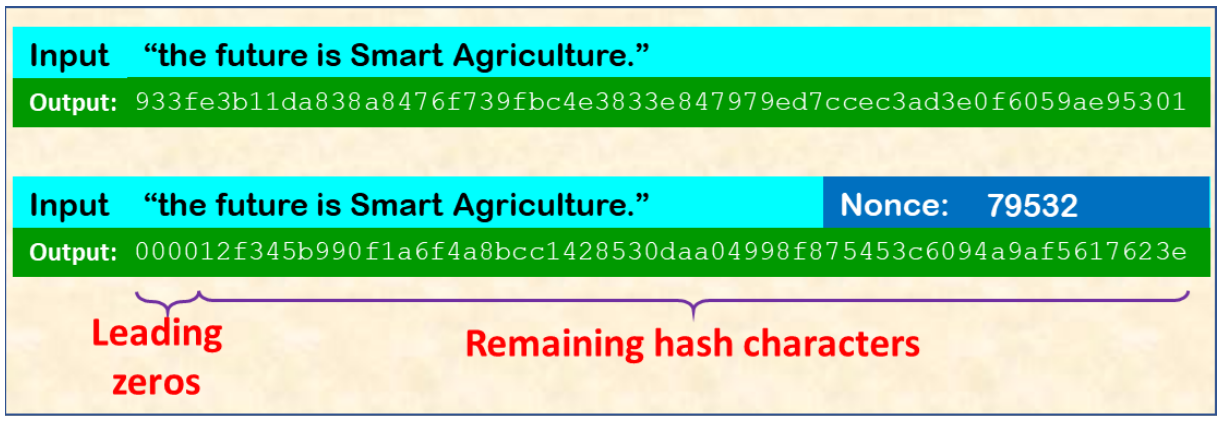

Figure 19. Changing the Nonce to get a number of target hash zeros.

The operation in which the correct Nonce is found to close the block is called **mining**. The number of target zeros increases the hardness of the puzzle. To find the Nonce that gives one zero you may need milliseconds. This amount of time exponentially increases if you require ten or twenty leading zeros. It

might need days or months of continuous work on an ordinary computer. That is why the miners require a lot of computing power to close each block. To overcome this problem, the miners used the advanced fast processors in the graphics cards called the graphical processing units (GPUs) instead of the usual central processing units (CPUs).

Once the block is closed, the Nonce is shared in the network with all other members; if they all accept it, it is called a Proof of Work (PoW), and the block is attached to the previous block. When several blocks are joined the same way, it is called the **blockchain**.

The blockchain

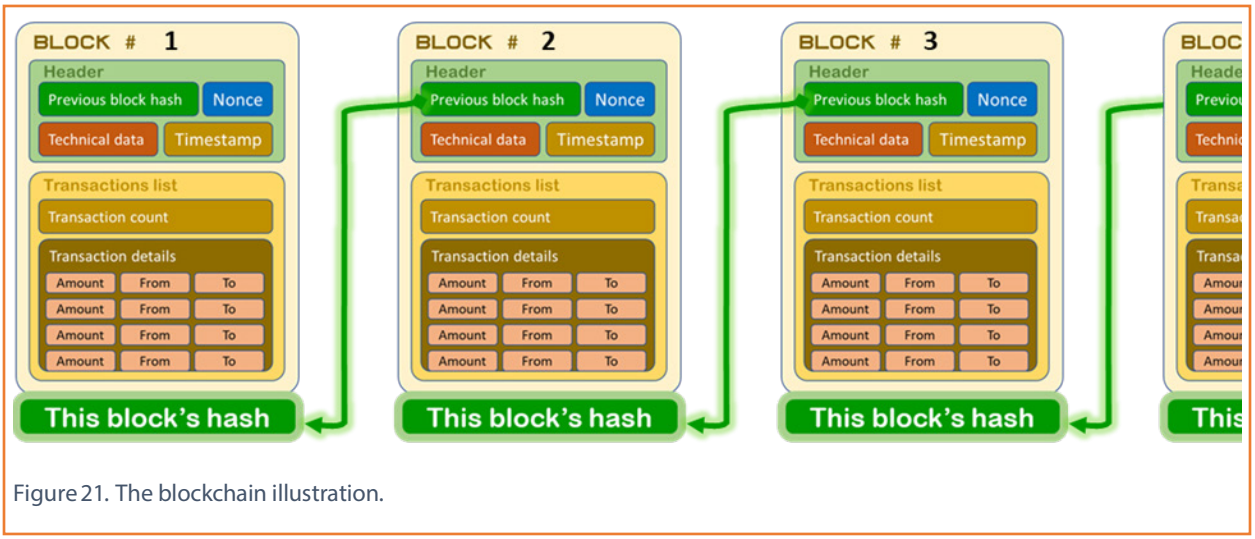

Figure 21. The blockchain illustration.

The blockchain is a series of linked blocks of data; each Block is sealed using a complicated hashing algorithm, where the hashed data include the previous Block's hash. Figure 4 shows an illustration of the Blockchain. As we see, Block #2 has the hash of Block #1 in its header, and Block #3 has Block #2 hash in his header, and so on. If by any means someone modified the data in Block #3, then its hash will change, so it will instantly be unlinked from the blockchain network because the "Previous block hash" written in Block #4 is different from the hash shown in the modified Block #3. The main feature of the blockchain is that it is duplicated with all the network members, so when someone modified Block #3, the chain will stop at #3 because #4 and all later blocks do not recognize the modified hash of # 3. So, when a new block needs to be added, it will search the tallest chain throughout the network, as it is probably the most trusted chain with consensus from all members.

As we see in Figure 5, the new blocks are constantly added to the longest chain. So, when someone modified Block #3 in the upper chain (one of the duplicates in the network), it has immediately been unlinked from its following blocks, losing its length and making it less attractive to the new blocks. Sometimes, two miners add their blocks to the longest chain simultaneously, so the top of the chain has two heads instead of one. In this case, some miners consider one of the blocks the last block, and the others consider the second one, then the chain continues to grow on both sides. In that case, the wing that spent more energy to mine (the more complex blocks to seal) is considered the winner, and the other wing is invalidated from the network.

As it appears, the transactions are securely stored in the blocks, and the blocks are securely linked to the blockchain. The blockchain is duplicated and distributed to all the network members (peer-to-peer transmission). It is easy for any member to search for any transaction in the blockchain because the blocks are linked as one table. A secure ledger is finally in his pocket, without the need of a third party. That is why this technology is named the distributed ledger technology. It is worth saying that the blockchain arrangement is one of many arrangements that the blocks can be placed and verified. Other arrangements include Hashgraph, Directed Acyclic Graph (DAG), Holochain, Tempo (Radix), and Tangle technologies (188,189), describing each type is beyond the objectives of this work. Thus, it is more practical to refer to this technology as DLT, not as blockchain

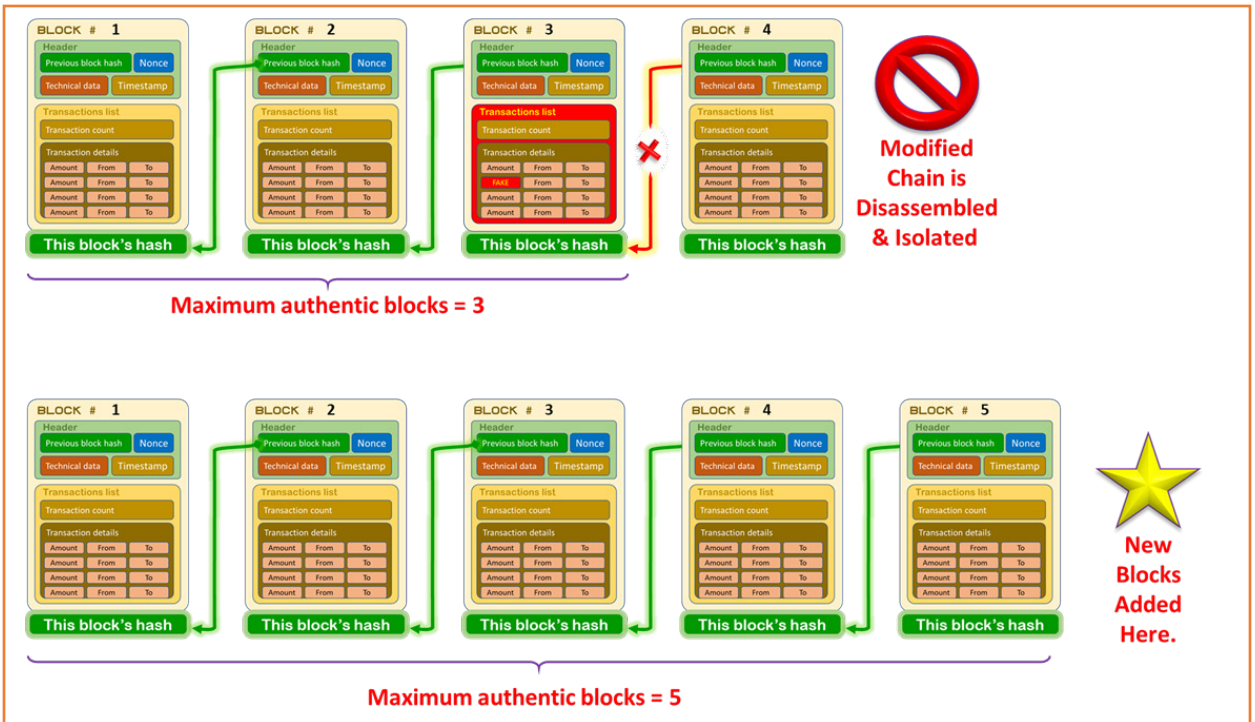

Figure 22. Modifying a bloch unlins it from the chain and prohibits new blocks from been added to its chain. New blocks are added to the tallest chain.

Smart contracts

In real-world trades, some merchants need to perform conditional transactions; If "A" bought some supplies from "B", but he did not pay the price in full, he made a 30% down payment, then after the supplies arrive at the warehouse of "A", he transfers the remaining 70% to "B". In this case, "A" paid 30% without receiving anything, and "B" shipped the supplies before receiving his remaining money. This transaction only happens when there is mutual trust between the parties or when there is a guarantor or a third party that guarantees the implementation of each party's obligations and punishes him for breaching them through litigation and the force of law.

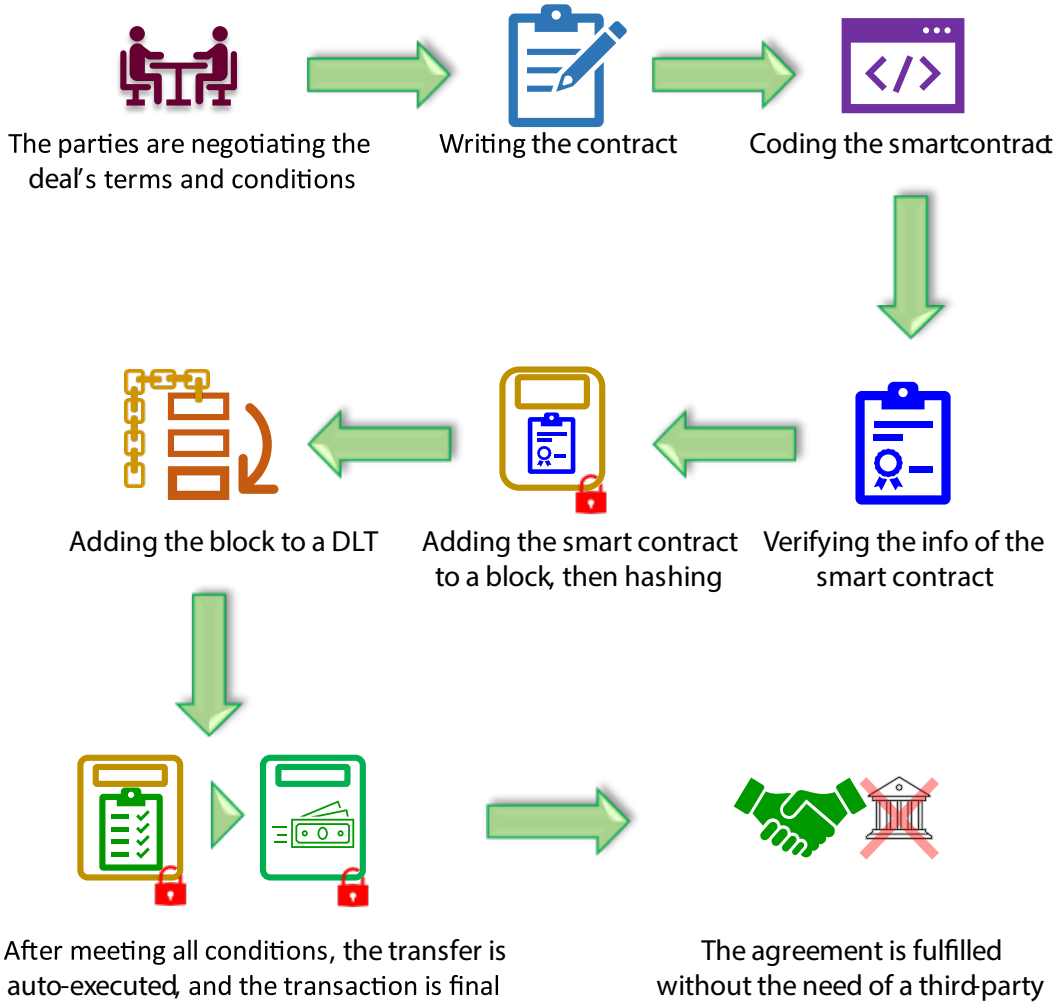

Figure 23. How smart contrancts work from agreement to execution without a third-party.

To omit the third party, DLT technology has solved this problem. Instead of logging this deal as a simple transaction, the deal is recorded as a conditional transaction. The conditional transaction includes each party's assets and obligations, in addition to the conditions in which each payment share is transferred from one side to the other. This extended transaction is called the smart contract. The smart contracts were popularized by the Ethereum network in 2016 (190). The smart contracts are stored in the blocks

like the usual transaction, and they are hashed and sealed to be immutable as well. Once the Smart Contract conditions are met, verified, and entered into the blockchain, the action occurs. This action includes transferring the corresponding payments automatically, without requiring a third party to confirm the process or judge between them in case of conflict. An illustration of the idea of smart contracts is shown in Figure 6.

Public vs. private blockchains

We discussed the concept of DLT, where the ledger and all its transactions are open to the public to read and write (after some digital confirmations). Copies of the ledger are stored with every contributor to the chain. This operation applies to cryptocurrency platforms like Bitcoin and Ethereum, which are considered public and open. 'Public' means anyone can contribute (permissionless network), and 'open' means anyone can search and read the transactions. However, in some applications, some applications need more security that only specific parties can add to the chain, and few parties can read or search the records, like military applications and tax records. Thus, private blockchain technology can solve this problem. Several platforms work with this concept, like Hyperledger and Corda. The military and Tax applications are private and closed. 'Private' means not anyone can contribute nor write (permissioned network), while 'closed' means not anyone can read or search; only the blockchain owner can read and track transactions for confidentiality and security.

On the other hand, some frameworks need to be private but open, like the supply chain platforms, where only suppliers, transporters, and retailers can contribute to the network. At the same time, everyone can read the ledger to trace and track the origins and properties of the products from farm to fork. Finally, some platforms are public but closed, like the voting blockchains, where anyone can vote, but only specific people can access and count votes (191).

DLT applications in the agriculture sector

The DLT technology offers a secure, decentralized method of storing transactions with the ability to retrieve data from any linked block by any member of the network. However, the stored data do not need to be monetary transactions; any text can be stored and tracked the same way. In 2017, There were multiple proposals to expand DLT usage beyond the financial services, i.e., to store medical records, voting records, real estate trades, supply chain operations, and many other applications (192,193).

In the field of agriculture, the DLT has many applications. At the top of these applications are the food traceability and food supply chain applications. Other applications include but are not limited to agricultural insurance, farm management, Agricultural IoT optimization, land registration, and e-commerce of agricultural products (194).

DLT in the food supply chain

The food supply chain applications of DLT started in October 2016 by Walmart retail company in the USA together with IBM. They started with only one product, the mango. They entered all the data about the mango, from farm to shelf, through a blockchain traceability system. They found that the blockchain

dramatically reduced the time needed to track any piece of information about the product, from 7 days (using traditional databases and unlinked sources) to 2.2 seconds using the Hyperledger Fabric blockchain (195).

Starting in 2019, Walmart announced that all its leafy greens suppliers must use the blockchain system in storing their product data. Following Walmart, many other food companies, like Nestle and Unilever, started to use the blockchain traceability system. The Hyperledger Fabric is an open-source private blockchain framework that fits a wide range of industries, including food supply chains.

The food-tracking blockchain network stores not only financial transactions, but the condition of the food while transported from place to place i.e., from farm to factory, or from the factory to store, and so on. The logged data include the ambient temperature and humidity, some chemical and physical properties of the products like sugar content, all the operations in the farm are logged too, like the type and vendor of the seeds, amount and types of fertilizers and pesticides. A typical food supply chain tracking using DLT is shown in Figure 7.

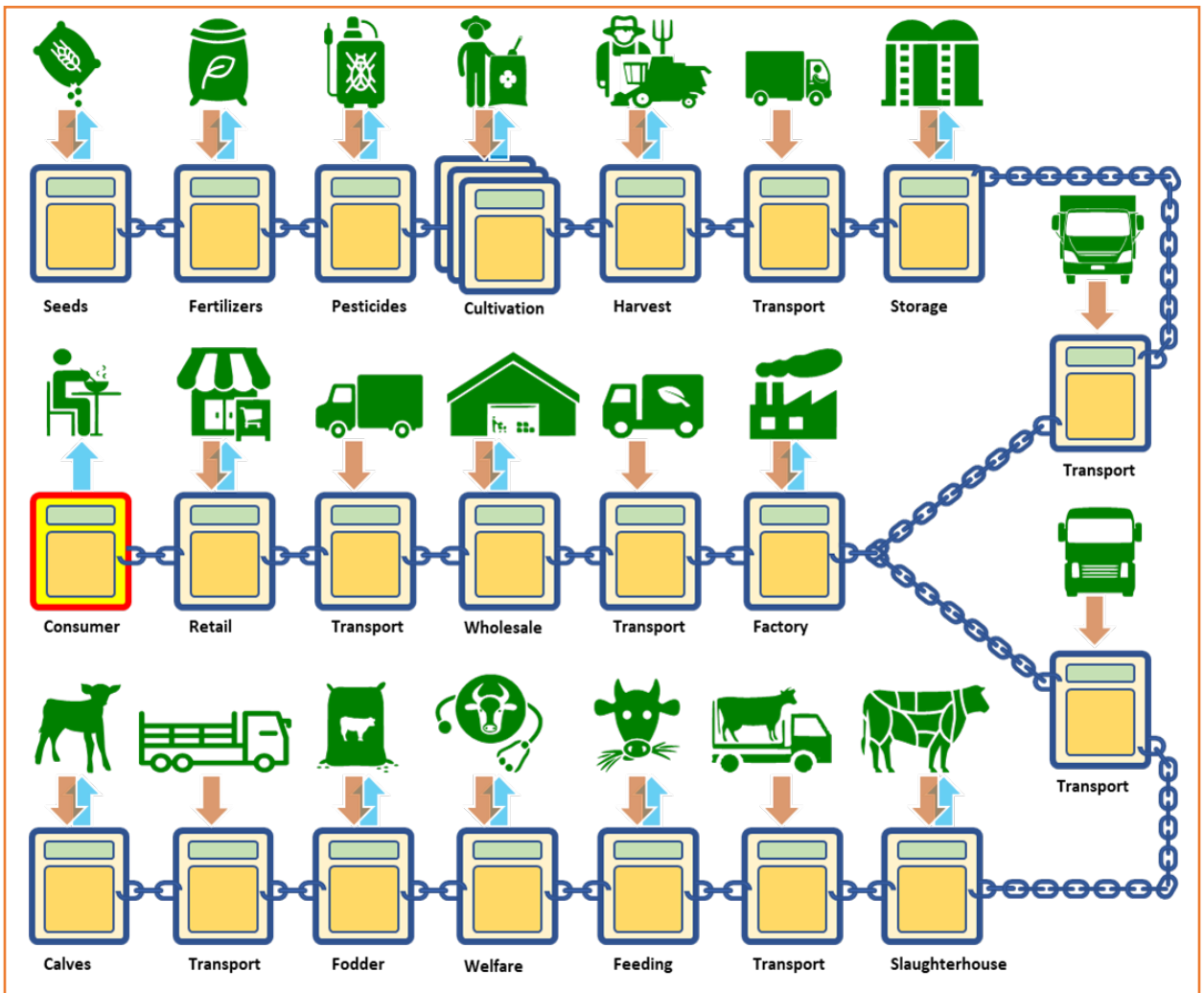

Figure 24. Food suply chain tracking using DLT for crops and livestock. Some paricipants have write-only (brown arrow), read-only (cyan arrow), or write-read previlages.

Figure 7 shows an example of a private blockchain for cereals and meat from farm to consumer. The cereals' journey starts from seeds selection and purchase. All the seeds' properties such as type, size, density, moisture content are logged to the blockchain network. Then the required fertilizers and pesticides are logged (quantities, types, and timestamps). In the field, all the farming processes are logged during the growing season till the harvest time. The physical properties of the crop are logged at harvest. Then follow-up logs are made during transportation to the storage silos, as well as all transportation events (to factories, to the wholesale or retail stores).

In the livestock path, we start with calves, logging their origin, age, and health measures to the blockchain. All the fodder properties, animals' welfare, animal care events, and feeding timetables are all logged until the end of the animal's life in the slaughterhouse, then transporting the meat to factories.

According to the example diagram in Figure 7, the transport processes are all write-only to the blockchain. The final consumer has read-only access, while all other nodes have write-and-read privileges.

Benefits of DLT food tracking

The characteristics of the DLT are believed to benefit the agricultural sector, especially the small-scale farmers. Small-scale farmers can benefit a lot from the intermediation reduction using smart contracts. Also, the connectivity to the whole supply chain can help them get fair prices for their produce. Additionally, the transparency of origination could remove the need for the traditional product certification, which will cut off its costs (196). We showed that using DLT in the food supply chain helps reduce the time and money for tracking food origin for large-scale retailers and small-scale farmers. Large-scale farmers can combine the benefits of both parties, thus, to gain a better reputation for their products, reduce the costs, and improving the production workflow.

One of the world crises in 1997 was the Mad Cow Disease (formally known as BSE) in the UK. The disease was first known in 1986, and the scientists tried to know the origin of the disease for years until they realized that the cause of the disease is the fodder of the cattle that contains proteins from dead animals (known as the meat and bones meal, MBM). This outbreak resulted in banning all beef imports from the UK worldwide for more than three years. What if we were then using the blockchain to trace the origins of foods? Scientists would have known the cause of the disease faster by comparing the diets of infected and uninfected cattle. Importers would have known which cattle were affected by the diseased diet and which ones were eating a healthy diet. We would not need to ban the import of meat from an entire country, and the ban would have been confined to some farms and not others. The same example applies to other epidemics like the swine flu in 1998, the foot-and-mouth disease in 2001, and other food-related pandemics (197).

Additionally, trustful food tracking by DLT help build trust in foods and dispel fears of unhealthy additives in foods. These unhealthy additives include additives in livestock feed, hormones and antibiotics given to poultry, and fertilizers and pesticides sprayed on plants. Even irrigation water used by some farmers may be contaminated with heavy metals and toxic factory waste, which is transmitted to the plant and from it to humans. All these hazards are in the production stage (cultivation and breeding). During the manufacturing process, the matter is much more comprehensive and dangerous, as there are dozens of flavors, additives, and preservatives which carry substantial risks to human health. During transportation operations, temperatures or the transportation environment may be

unsuitable and contribute to the spoilage of agricultural products, whether before or after processing. As for the long transportation distance, it may cause deterioration in some nutritional contents such as sugar in sugar cane. As for the wholesale and retail stores, the storage and display conditions may be marred by many faults that lead to product ruin or deterioration of their qualities.

All these characteristics can be known in detail through automated tracking using blockchain technology. The customer can know the amount of fertilizers used in plant production, the components of animal feed, and the conditions of storage, transportation, and distribution of all these products. This operation raises the consumer's confidence in what he eats and does not pose a danger to him or his family.

Agricultural insurance

Agriculture is a high-risk industry. Farmers are exposed to many unexpected risks that cause considerable losses to the crop, up to its total loss or the loss of a large percentage of it. Most problems arise because of unsuitable weather conditions such as frost waves, storms, and heavy rain. These events push farmers to cover their crops and livestock by insurance contracts. Conventionally, when risks occur, insurance companies estimate the risks and compensate the insured to the extent appropriate to his loss according to the agreement. Recently some insurance companies have started index-based insurance (IBI); This type of insurance does not look at each farmer's case individually. Instead, it looks at the entire region where the farm is located and monitors the temperatures, wind speed, and rain. For example, if the temperature drops below a certain degree thought to cause damage to the crop, the company pays all farmers in the area equally. The payment amount depends on the potential loss of the crop. Regardless of whether the damage occurred or not, the degree of damage was as estimated, less, or more. The same is true if heavy rains occur, which is feared to affect the crop, or if strong winds occur, thought to be uprooting a percentage of the plants, and so on.

This system depends only on meteorological measuring devices, and the companies do not incur the expenses of inspection and assessment for each case. The farmer does not have to submit a request for compensation nor to prove damages. All of the compensation is done according to all-inclusive standards. The IBI system is easy to feed into smart contracts, where monitoring devices are connected to the Blockchain and feed the values of temperature, wind, and rain. If one of the values reaches a threshold limit, it triggers the transaction condition in the smart contract, so the amount of insurance is immediately transferred to the farms connected to the network. This transaction happens completely automatically without a third party between the insurer and the insurance company.

Combining the DLT with IBI has been proved to resolve the problems of agricultural insurance and facilitates the development of innovative insurance mechanisms that benefit both small-scale and large-scale farms (198,199)

Smart farm management

Smart farming involves using IoT technologies that generate, store, and analyze a vast amount of data. In the IoT chapter in this book, we talked about cloud storage of data. Cloud storage is safe, fast, and highly accessible; however, it is an administrated operation; the cloud servers have hosts and administrators who can revoke the access to the data or can change its accessibility by adding more fees or limiting the bandwidth. Additionally, the cloud servers are subject to cyber-attacks like Denial-of-Service (DoS), Man-in-the-Middle (MitM), and other types of attacks. Besides, the hosting company can

go out of business at any time. All these hazards make us think about a more secured data storage that is free of the third party, which is the DLT. Distributing data to many locations (via DLT) makes it more secure and less dependent on one or more parties who administer the data or control its flow (199). However, there are some limitations and obstacles that will be detailed in section 3 below.

e-commerce of agriculture products

E-commerce is based on purchasing goods after viewing them online. This preview includes written descriptions, images, videos, or 3D previews via augmented reality technologies. After the inspection, electronic payment is made, and the goods are shipped to the customer. The main problem in this process is the confidence in the accuracy of the information provided by the merchant. This lack of trust made some stores provide a system of payment upon receipt and after the actual inspection, and this, in turn, caused a problem for the merchant for fear of rejecting his goods after incurring shipping costs.

This problem is increasing in agricultural products more and more, as the quality of the products changes during shipment. Therefore the customer will receive something other than what he has seen. Also, some commodities cannot verify their specifications by regular inspection. When purchasing a piece of clothing, for example, the customer may request a specific size, a specific color, and a specific design. All of this can be inspected and confirmed upon receipt. However, what about fruits? How can you be sure that they are organic, for example? How can one be sure that the country of origin is the country Doe? Moreover, how to ensure that the trees were irrigated with clean river water, not polluted water? All of these are difficult to verify upon receipt, except by conducting laboratory analyzes that are costly in money and time consuming as well.

When using the blockchain, all the transactions that took place for the crop are recorded. Additionally, the types of fertilizers and pesticides and their quantities are all recorded. Even the weather conditions at germination and the country of origin are recorded in the network. This system gives the customer full knowledge of the crop he is buying and the extent of the merchant's truthfulness in the information he has told him about the crop. On the other hand, when signing smart contracts between farms and supply chains, each party guarantees its material rights, as money is transferred to it automatically upon delivery of the products with the required specifications.

This technology, if it is generalized, provides the opportunity for small farms to take their opportunity on an equal footing with large farms, as well as the opportunity for developing countries to export their products conveniently. Importing countries know the origins and conditions of cultivation of the crops they consume with complete transparency.

Challenges and obstacles

The distributed ledger technology enables reliable and secure data transactions that open new horizons of data-driven applications for smart agriculture. However, there are a lot of challenges and obstacles that face the spread of this promising technology.

Sources' reliability

Some of the challenges depend on one of the benefits of the DLT, which is immutability. DLT ensures that data has not been altered by any means. However, what if the data has a mistake? No one can correct it! This problem worsens with the IoT-based DLT, i.e., if the data is added to the blocks by machines or sensors, the DLT will hold the inputs as is. This immutability is good to ensure data trustfulness, mainly when the sensors record fruits properties. The problem occurs when there is any trouble with this sensor's readings. The trouble is either with technical malfunction or with cyberattacks of any kind that alters its reading. The problem inflates when this inaccurate data is linked to a smart contract that may accept or reject the product quality and consequently pass or hold the associated financial transactions. This challenge is vital, because the transactions in the blockchain are final and irreversible unless by the consensus of all parties. This problem puts it on our shoulders to ensure the accuracy and reliability of all devices connected to the network, as well as to periodically check that the entered data matches reality (190,200).

Integration and compatibility

The DLT is an emerging technology that is still immature. There are still many architectures of the networks, many consensus algorithms, and many other details of the technology that make the different networks incompatible with each other. The problem is that currently, there are tens of competing organizations, each developing its own technology standards. On the other hand, there are some efforts to solve the incompatibility problem like the Hyperledger Fabric and R3 Corda that aim in allowing interfaces between multiple DLT systems and allow transactions and id-validation between counterparts (201). Luckily, most agricultural applications currently depend on Hyperledger Fabric which supports a wide range of frameworks, ensuring better compatibility and interoperability.

Technical barriers

Like all modern technologies, DLT requires a reliable hardware infrastructure and workforce technical skills. Additionally, DLT requires reliable internet connections to allow consistent operation of the system. Before applying the DLT, the society and the stakeholders must have sufficient awareness of the importance of the technology, the method it works, and the skills needed to make it function as intended. This requires training and education of all the involved persons in the system (202).

Other problems

DLT frameworks are either public or private. Most of the agricultural DLTs are private and permissioned networks to ensure that the involved members only are allowed to write or read to the system. There are some confidentiality concerns about exposing the selling prices or even the suppliers' identities which sometimes need to be confidential. This problem might be solved by encrypting the suppliers' identities (through pseudonyms linkage) and selling prices, making it readable only to authorized parties (203).

The initial setting of the DLT framework takes a lot of time, money, and training. Then, it needs maintenance and follow-up to ensure flawless operation (190).

Although DLT can benefit both small-scale and large-scale farmers in e-commerce and supply-chain integration, the costs and problems would be more considerable for small-scale farmers to be integrated into the DLT system. Thus they might need some government or organizational support at the beginning (199).

It needs more efforts to establish DLT governance rules, especially in the absence of a central entity. These governance rules should solve several problems, like data authorship, blockchain fork problem, incorrect data entries correction, and other minor challenges in reference # (201).